2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)

Conference Venue: University of Electronic Science and Technology of China, Sichuan Province, China
Conference Dates: Dec. 18-20 2020

Organizers:
University of Electronic Science and Technology of China (UESTC)

Sponsors
The National Natural Science Foundation of China (NSFC)
National High Technology Research and Development Program of China
China International Talent Exchange Foundation

Technically Co-sponsors:
IEEE
IEEE Chengdu Section

2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)

is published by the Institute of Electrical and Electronics Engineers, Inc. and printed by the UESTC Press, Chengdu, 610054, Sichuan, China in December 2020.

IEEE Catalog Number: CFP20WAM-PRT
ISBN: 978-0-7381-4257-9

Preface

Recently, the United States and China have made great progress in the field of quantum computing and quantum computer research. This year, China has won major victories in landing on the moon and fighting COVID-19, some leading information technologies have played an important role. Up to now, Strong network and computing power has brought great convenience to our work, study, and life.

In order to stimulate the future development, explore novel applications, exchange ideas, and express opinion, the 2020 17th IEEE International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP2020) will be held at University of Electronic Science and Technology of China (UESTC) in Chengdu on December 2020. The aim of this conference is to provide a good forum for teachers and researchers working on both theory and applications on computer science, artificial intelligence, machine learning, big data, cloud computing, wavelet analysis, active media technology and information processing.

This conference is following the success of the series former conferences from the first conference in 1999. The ICCWAMTIP2020 emerged as a leading conference on new computing architectures and new information processing algorithm. We have received a lot of full papers submitted from all over the world. To ensure the quality of the conference and proceedings, each paper was reviewed by different reviewers. After a thorough review process, the program committee and academic committee selected final papers as regular papers and short papers. These papers cover wide range, such as computer science, wavelet analysis, active media technologies, information security, bioinformatics, sensor network, AI, BI, ANN, Big Data, cloud computing, Internet of things (IoT), and so on. The papers study the hot issues in their researching fields, present many valuable ideas. The proceeding of ICCWAMTIP2020 was published by UESTC Press. There are some invited talks delivered by distinguished researchers in the world. We must add that the conference organizing committee, the conference program committee, the conference academic committee and the reviewers did most excellent job within a very tight schedule.

We wish to thank all the authors for submitting their work to ICCWAMTIP2020 and all the participants, whether you came as a presenter or an attendee. We hope that there was ample time for discussion and opportunity to make new acquaintances, and you experienced an interesting and exciting conference and enjoyed your stay in Chengdu. We hope that all of you will enjoy and benefit from the papers in this book.

The ICCWAMTIP2020 was supported by the Scientific Research Project of Ministry of Science and Technology of P.R.China, the National Natural Science Foundation of China (Grant No.61370073)，the National High Technology Research and Development Program of China (Grant No.2007AA01Z423), New Century Excellent Talent Support Project of Chinese Ministry of Education, the Scientific Research Project of Sichuan Province, the Scientific Research Project of Chongqing

Municipality, the Scientific Research Projects of Chengdu Civil-Military Integration Project Management Group, Chengdu Chengdian Network Technology Co., Ltd., Sichuan Yin Ten Gu Technology Group, Chinese Computer Association, State Administration of Foreign Experts Affairs of P.R.China, China International Talent Exchange Foundation, Doctor Station Foundation of Chinese Ministry of Education, IEEE Chengdu Section.

Jian Ping Li, Ph.D., Professor
Dean of Big Data Research Institute
Founder and Editor in Chief of International Progress
on Wavelet Active Media Technology and Information Processing
Head of International Centre for Wavelet Analysis and Its applications
School of Computer Science and Engineering
University of Electronic Science and Technology of China（UESTC）
Emails: jpli2222@uestc.edu.cn, 1073075862@qq.com
December, 2020

CONFERENCE ORGANIZATION

International Advisory Board:

Mo Jamishi, UT Dallas, USA
Bruno Torresmi, Fance
Yuan Yan Tang, University of Macau, Macau, China
Yong Zeng, UESTC, China
Cai Dong Xiong, UESTC, China
Hong Bing Xu, UESTC, China

Honored Chairs:

John Daugman, Cambridge University, UK
Simon X. Yang, University of Guelph, Canada
Guang Nan Ni, Chinese Academy of Sciences, China
Nan Shan Zhong, Guangzhou Medical University, China
Chao-Hsing Hsu, Chienkuo Technology University, Taiwan, China

General Chairs:

Jian Ping Li, UESTC, China
Ishfaq Ahmad, University of Texas at Arlington, USA
Clarence De Silve, UBC, Canada

Editor in Chief:

Jian Ping Li, UESTC, China
Xin Shuo Li, Chengdu Polytechnic College, China

Co-Editors:

Igor Bloshanskii, Moscow State Regional University, Russia
Ishfaq Ahmad, University of Texas at Arlington, USA
Simon X. Yang, University of Guelph, Canada

Steering Committee Chairs:

Lionel M. Ni, The Hong Kong University of Science and Technology, Hong Kong
Victor Wickerhauser, Washington University, USA
Jim X. Chen, George Mason University, USA
Rajkumar Buyya,The University of Melbourne, Australian
Heng Tao Shen, UESTC, China
Guang Jun Wen, UESTC, China

Program Committee Chairs:

Xiaobo Yuan, Windsor U, Canada
Di Liu, UESTC, China
Jie Lin, UESTC, China
Feng chun Tian, Chongqing University, China
Yi Chai, Chongqing University, China
Hong Ma, Sichuan University, China
Mao Kang Luo, Sichuan University, China
Si Hao Huang, Sichuan University, China

Organizing Committee Chairs:

Gauri S. Mittal, U of Guelph, Canada
Bo Fu, UESTC, China
Xing Zheng Ai, UESTC, China
Fan Yang, UESTC, China
Yangyang Wang,UESTC,China
Shikai Sui, UESTC, China
Yuan Gao, UESTC, China
Ruinan Shun, UESTC, China
Tiankai Li, UESTC, China

Finance Chairs:

Xiaofeng Gu, UESTC, China
Wen Yan Jiang, Chengdu Chengdian Internet Technology Co., Ltd, China
Tao Song, Aoxin Technology Co., Ltd, China
Xi He, UESTC, China
Yue Zhou, UESTC, China

Publication Chairs:

Stefano Gregori, University of Guelph, Canada
Qingtao Xue, UESTC, China
Jiudong Yang, UESTC, China
Gaofeng Zhao, UESTC, China
Mudassir Khalil, UESTC, China
Tiankai Li, UESTC, China
Yuan Gao, UESTC, China
Amin UI Haq, UESTC, China

Publicity Chairs:

Chunyi Su, Concordia U, Canada
Yuehao Yan, Chengdu Technological University of China, Chengdu, China
Yujun Yang, UESTC, China
Xinshuo Li, Chongqing University, China
Fadia Shah, UESTC, China
Qiangqiang Cheng, UESTC, China
Tengqiu Yu, UESTC, China
Haoyang Chang, UESTC, China

Registration Chairs:

Qingsong Wang, UESTC, China
Fei Xiao, UESTC, China
Shunli Li, UESTC, China
Zhilong Lai, UESTC, China
Bless Lord Y. Agbley, UESTC, China

Conference Network Chairs:

Sheng Jiang, UESTC, China
Tao Jiang, UESTC, China
Fei Xiao, UESTC, China
Jianguo Zhang, UESTC, China
Abida Sharif, UESTC, China

Table of Contents

Content of Proceeding of 17th ICCWAMTIP

Track 01: Theory and Experiment

Track 02: Multimedia Technology

Track 03: Embedded System and Others

RESEARCH ON WAVELET ANALYSIS AND HILBERT SPACE

Yuan Yan Tang, Ph.D., Professor
Department of Computer and Information Science, Faculty of Science and Technology
University of Macau, Macau, China

Abstract:

1. Wavelet Analysis and Its New Progress
2. Normed Space and Inner Product
3. Bannach Space
4. Hilbert Space

Biography:

Yuan Yan Tang is a Chair Professor in Faculty of Science and Technology at University of Macau and Professor/Adjunct Professor/Honorary Professor at several institutes in China, USA, Canada, France, and Hong Kong. His current interests include wavelets, pattern recognition, image processing, and artificial intelligence. He has published more than 400 academic papers and is the author/coauthor of over 25 monographs/books/bookchapters. He is the Founder and Editor-in-Chief of International Journal on Wavelets, Multiresolution, and Information Processing (IJWMIP), and Associate Editors of several international journals. He is the Founder and Chair of pattern recognition committee in IEEE SMC. He has serviced as general chair, program chair, and committee member for many international conferences. Dr. Tang is the Founder and General Chair of the series International Conferences on Wavelets Analysis and Pattern Recognition (ICWAPRs). He is the Founder and Chair of the Macau Branch of International Associate of Pattern Recognition (IAPR). Dr. Y. Y. Tang is a Fellow of IEEE, and Fellow of IAPR.

THE SIGNAL PROCESSING OF SMART ANTENNA SYSTEM IN 5G COMMUNICATION

Chao-Hsing Hsu, Ph.D.
Professor, Department of Information and Network communication
Chienkuo Technology University, Taiwan, China

Abstract:

In the 5G communication, it asks for high quality and good efficiency. Base station antennas use omnidirectional or sectored pattern, which could cause the power waste in unexpected direction and interference for the others. In a smart antenna system, SDMA can allocate space to many users by using an angle separation and create a different beam for each user in the same frequency channel simultaneously. Each beamformer creates a maximum toward the desired one of its users while nulling the other users. Its spatial separation ability can avoid making interferences one another. Therefore, the system capacity can be increased. Smart antenna radiation patterns not only adjust maximize the main lobes toward the directions of the desired signals, but suppress interferences by placing nulls in the directions of interfering. A smart antenna system can make MIMO-SDMA optimization come true and satisfy the 5-G communication system.

Biography:

Professor Chao-Hsing Hsu received the B.S. degree in electrical engineering from Feng-Chia University in Taiwan in 1981, and derived the M.S. degree in electrical engineering from Florida International University, Florida, U.S.A. in 1992. Professor Hsu earned the Ph.D. degree in electrical engineering from Florida International University, Florida, U.S.A. in 2002, and at the same time he was elected as the Outstanding Ph.D. Graduate due to his dissertation. The dissertation topic of Professor Hsu is Optimizing the Radiation Pattern of Smart Antennas Using Genetic Algorithms. It's the 5G communication core technique. From 2002 to 2007, Professor Hsu took positions of associate professor and chairperson in Department of Electronic Engineering in Chienkuo Technology University in Taiwan. From 2009-2011, In Chienkuo Technology University, Professor Hsu took the position of professor in Department of Computer and Communication Engineering. From 2011 to 2019, and he took positions of Professor in Information and Network Communication Department and Director in Computer Center from 2011 till now. Currently, Professor Hsu serves as the Dean of Engineering College in Chienkuo Technology University.

His research has been focused in microstrip antenna design, adaptive antenna beamforming technology, smart antenna SDMA technology, optimization algorithm, microwave circuit design and cloud computing applications. Profess Hsu has held multiple leadership roles and awards in the university and academic communities. He

ever derived best paper awards in The Third International Conference on Innovative Computing, Information and Control ICICIC-2008, and also derived the best paper award in The Second International Symposium on Intelligent Informatics ISII-2009. He ever served as the Plenary Chair in The Fourth International Conference on Innovative Computing, Information and Control ICICIC-2009. Currently, Profess Hsu also served as associate editors in several international journals which are JIHMSP, IJICIC, ICIC Express Letters and ICIC Express Letters, Part B: Applications. As to his smart antenna system techniques in 5G communication, Professor Hsu obtained the Invention Patent of Taiwan in 2003 and the Invention Patent of USA in 2008. By using his invention patent, Professor Hsu also got a Gold Medal Award of Merit at INPEX 2011 which is an international invention exhibition held in U.SA. and a Gold Medal Award of Merit at INVENTECO 2012 which is a world invention exhibition held in Italy.

THE NEW INFORMATION TECHNOLOGY AND ITS APPLICATIONS TO SARS & COVID-19

Nan Shan Zhong, Academician of Chinese Academy of Engineering,
Professor of Guangzhou Medical University, Guangzhou, China

Abstract:

1. Artificial Intelligence
2. Block Chain
3. Big Data
4. SARS
5. COVID-19

Biography:

Nan Shan Zhong (born In October 1936), male, born in Nanjing, Jiangsu Province, graduated from Beijing Medical College, academician of the Chinese Academy of Engineering, famous respiratory expert, Medal winner of P.R.C., the dean of current national respiratory system disease clinical medical research center, director of high-level expert group of the National Health Commission of P.R.C., national health science expert. He engaged in the medical and teaching and scientific research of respiratory medicine, expertise for chronic obstructive pulmonary disease and other respiratory disease, he is China's leader of fighting against atypical pneumonia (SARS) and COVID-19. In November 2020, he won the 2020 annual achievement award of He Liang He Li fund of science and technology, on December 15, 2020, he was awarded the honorary doctorate from the Hong Kong Polytechnic University.

RESEARCH ON SECURITY THEORY OF MILITARY THINKING SPACE BASED ON QUANTUM TIME-SPACE

Jian Ping Li, Ph.D., Professor
International Centre for Wavelet Analysis and Its applications
Big Data Research Institute, School of Computer Science and Engineering
University of Electronic Science and Technology of China（UESTC）
No. 2006, Xiyuan Ave., West Hi-Tech Zone, 611731, Chengdu, Sichuan, China
Emails: jpli2222@uestc.edu.cn, 1073075862@qq.com

Abstract:

1. Fourier Analysis
2. New Wavelet Analysis
3. Cyberspace Security
4. Quantum Time-Space

Biography:

Professor Dr. Jian Ping Li, male, born on October 11,1964. He received the B.S. degree in applied mathematics from Chongqing University, Chongqing, China, in 1986, the M. Eng. degree in software engineering and M. Sci. degree in computational mathematics from the Graduate School of Xi'an Jiaotong University, Xi'an, Shanxi, China, in 1989, and the Ph.D. degree in computer science from the Graduate School of Chongqing University, Chongqing, China, in 1998. From 1999 to 2000, he was a post-doctoral and visiting professor working at Hong Kong Baptist University under the leadership of Professor Dr. Yuan Yan Tang. From 2002 to 2003, 2005 to 2006, and in 2010, 2011, 2013, 2014, 2015, he was a senior visiting professor working respectively at Provence University, France, University of Guelph, Canada, Washington University, USA, University of Zurich, Switzerland. He is presently a Professor in International Centre for Wavelets Analysis and Its Applications (ICWAA) of University of Electronic Science and Technology of China（UESTC）, Chengdu, China, and as a head of ICWAA, he is the dean of Big Data Research Institute of UESTC. Dr. Li has served as a Syndic for Awards of National Science and Technology of China, a founder of the International Journal on Multiresolution, Wavelets, Applications (IJMWA), a founder and Editor in Chief of International Progress on Wavelet Active Media Technology and Information Processing, and as General Chairman of many

international conferences, a reviewer for many international famous Journals. His book Wavelet Analysis & Signal Processing: Theory, Applications & Software Implementations, was awarded the second prize of National Science and Technology of China (1999), and it is very important reference for many scientists. Dr. Li has published more than 300 technical papers and is the author/ co-author of 30 books on subjects ranging from wavelet analysis and its applications to computer science. His current interests include wavelet theory and applications, fractal, image processing, pattern recognition, information security, big data, artificial intelligence.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, the project of Science and Technology Department of Chongqing Municipality, Chengdu Chengdian Network Technology Co., Ltd., Chengdu Civil-military Integration Project Management Co., Ltd., and Sichuan Yin Ten Gu Technology Co., Ltd.

LINK-ADAPTIVE WAVELET OFDM FOR FUTURE MOBILE COMMUNICATION

MORDECAI F. RAJI[1], JIAN PING LI[1], AMIN UL HAQ[1]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China
E-MAIL: mraji@qq.com, jpli2222@uestc.edu.cn

Abstract:

The increasing demands and requirements of mobile communication are gradually rendering the numerous current waveform designs obsolete. For example, in the realization of 5G, several waveforms are proposed. These waveforms are promising, but not without their respective drawbacks. Considering the ever-increasing demands, these drawbacks might make them unsuitable in higher generations of mobile networks such as 6G. Wavelet-based waveforms are considerable alternatives in meeting the ever-growing demands of future mobile communication. In this work, we investigate a wavelet Orthogonal Frequency Division Multiplex (WOFDM) algorithm that automatically adjusts to the constellation order according to the channel state. This we refer to as Link Adaptive Wavelet OFDM (LA-WOFDM). With this, we achieve a spectral efficient waveform while maintaining a balance in link quality. A spectral efficient waveform system yields higher power efficiency. Finally, our results show that Link Adaptive Wavelet-OFDM can compete with the state of the art.

Keywords:

Link-adaptive; Wavelet-OFDM; 5G; 6G

1. Introduction

Emerging mobile technologies will make possible a fully automated and remote management system. They are supported by the advancement of mobile generation networks; 5G drives the effective adoption of smart life; a commercial term used to describe the interconnection of millions of sensors embedded into materials, people, and environments. The classes are autonomous driving, immersive gaming, robotics and drones, Internet of Things, etc. Some of the emerging applications described above indicate that 5G operates with a high degree of diversity in terms of requirements and services. Some of these requirements, relative to 4G, are characterized by high spectral efficiency, multi-gigabit-per-second (Gbps) data rates, high spectral efficiency, low latency, high mobility, and high connection density. Lately, the increasing number of certain new-sprung applications, as well as yet to be conceptualized applications will require improved Quality of Service (QoS) higher than what 5G can offer [1]. To combat 5G limitations, research directions are outlined in [2].

A close look at wireless systems architecture reveals that waveform plays a key role in physical layer solutions and it is centric to the overall efficiency of a mobile communication system. In a broad form of explanation, the performance of a wireless system depends largely on the radio access technology. It is a determinant of different parameters. Such as robustness against channel impairments, Transmission (Tx) and Reception (Rx) energy efficiency, data transfer rate, and compactness of symbols in the time-frequency plane. This paper is therefore focused on the design of an efficient waveform.

This work is structured as follows: Section 2 highlights the existing research contributions relating to this paper; Sections 3 describes the major contributions of this proposed work; Section 4 gives the detailed system description, setup and simulation of this work while Section 5 brings this work to conclusion.

2. Background of related work

OFDM simple design makes it an easy choice for wireless systems engineers. This is also evident in the waveform selection for 5G release 15. Amongst the proposed waveform, the International Telecommunications Union chooses Cyclic Prefix OFDM (CP-OFDM) for downlink and Single-Carrier OFDM (SC-OFDM) for uplink. Aside simplicity of the OFDM waveform, other reasons are that the wireless societies are familiar with OFDM's use including in 4G LTE and other standards. Therefore, we can conclude it is a mature technology. The technical attempts at mitigating OFDM's drawbacks result in the evolvement of OFDM to other waveforms. These drawbacks are not limited to high PAPR, sensitivity to Carrier Frequency Offset (CFO) and Out of Band (OOB) emissions, and reduction in transmission throughput due to cyclic prefix inclusion. A distinct approach is the Discrete Wavelet Transform (DWT) in OFDM. This is

generally known as OWDM. The application of DWT in signal coding was introduced in [3]. Some of the subsequent articles are [4] and [5]. The work reported in these references are narrow in scope and therefore do not provide enough guidelines in extending the results to application in future mobile communication. A broader scope of OWDM's application guidelines is provided in [6].

Link adaptive channel systems have been reported in several articles. [7] expands knowledge base by discussing adaptive transmission systems that share spectrum resources. In this scheme, users (primary and secondary) utilize Alamouti Orthogonal Space-Time Block Coding (OSTBC) system under mutually related antennas over Rayleigh fading channels. It derives expressions for the average spectral efficiency, average Bit Error Rate (BER) and outage probability of the system for each individual transmission technique. [8] reports a fairly different approach to reducing Peak To Average Power Ratio (PAPR) that are caused by nonlinear distortion in Radio Over Fiber (RoF) system. It modulates subcarriers with considerable distortion and suitably reduces the modulation level on the subcarriers to secondary levels. Results show this technique improves the BER performance significantly while the decrease in data rate for a system with 64 subcarriers and 16QAM as primary and 4QAM as secondary modulation levels is around 4%. A similar link adaptive 2 x 2 MIMO employed wavelet-OFDM-Radio Over Fiber is discussed in [9]. Diverse wavelets were incorporated to maintain small side-lobes and low PAPR resulting in high power efficiency. Specifically, the db1 wavelet in the orthogonal category and wavelets of order 1.3 in the bi-orthogonal (or reverse) category gives the best power efficient and spectral efficient transmission link quality. [10] explains the 5G base stations performance of adaptive modulation and coding based on the feedback from the user on channel state information. This improves the spectrum efficiency by selecting different combinations of code rates and modulation types.

3. Major contributions

The references discussed in section II are the various attempts at realizing a more spectral and power-efficient waveform suitable to meet the ever-evolving mobile generation network. The aim of this work is similar, however with a different approach. A careful look at the above discussed references shows that they are mostly limited to non-adaptive Wavelet-OFDM. [9] is adaptive but limited to RoF system. As stated above, this work aims to investigate and develop both an energy-efficient and power-efficient waveform while limiting waveform complexity. The fluctuations in the channel link quality (channel state) are high, so there is the need for a self-adaptive (to the current channel state), reliable and spectral efficient waveform system. The adaptive algorithm is designed based on the classic threshold BER algorithm under the assumption of perfect channel estimation for M-PSK modulation schemes. The results are compared to the non-adaptive scheme.

4. System description

For the purpose of coherency and sequential description of this work, effects of SNR variations on BER (under un-adaptive modulation order) are first discussed. Fig.2 shows the BER response to the varying SNR. An observation of the graph shows that at low SNR of around 0dB, constellation orders 16PSK to 128PSK have very close BER values. As the SNR increases the BER values gap widens. For example, for a given maximum BER value of $1x10^{-3}$, it requires a SNR value increase of about 5dB from QPSK to 8PSK, and roughly the same SNR value increase for the rest of the constellation orders.

Here, we present an end-to-end working principle of LA-WOFDM from the transmitter, through the channel, to the receiver. Firstly, User data-bits are mapped to a suitable constellation (M-PSK) order. The suitable constellation order is set to a minimum (QPSK) at default by the link adaption control subsystem. At this stage, the channel state is unknown. After mapping, the symbol-data is wavelet coded by convolution to generate a wavelet-OFDM signal. For the processing of received signals, this process is reversed. The link adaptation control subsystem in the receiver continuously updates the transmitter of the SNR data. With this, the transmitter and receiver subsystems select or switch modulation orders accordingly to maintain the BER below the specified threshold value of $1x10^{-2}$. The SNR values are defined in the link adaptation control as shown in Fig.1.

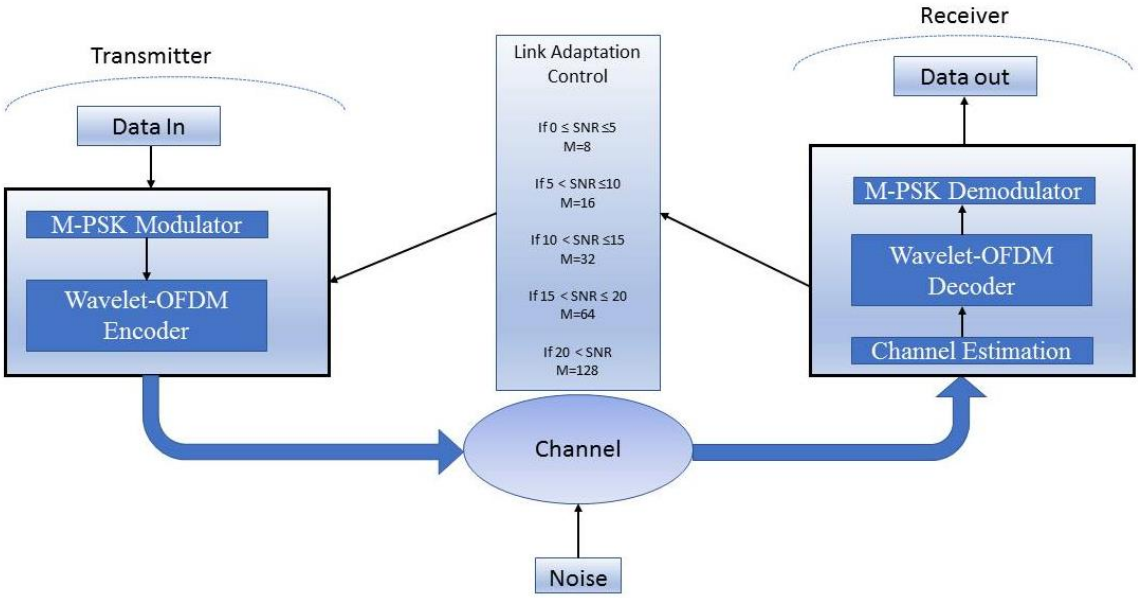


Fig.1 Schematic diagram of link-adaptive Wavelet-OFDM system

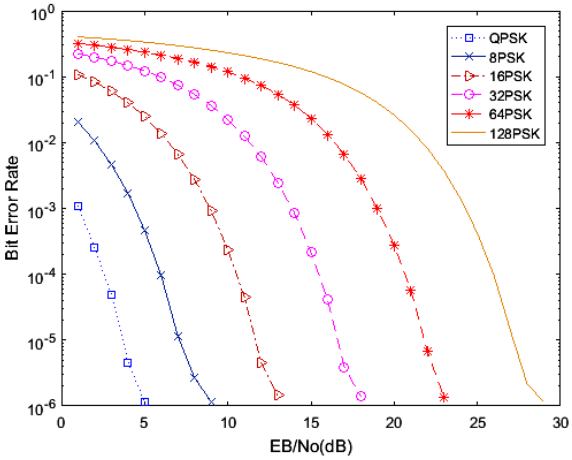


Fig.2 Haar Wavelet-OFDM with diverse PSK modulation orders

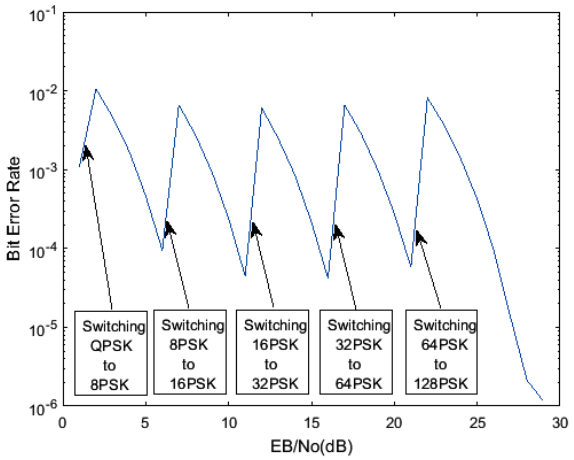


Fig.3 Haar Wavelet OFDM system with adaptive PSK modulation schemes as described in Fig.1

In fig.3, at QPSK order, the system targets the set maximum BER of $1x10^{-2}$. It peaks at 2.5dB. Further increment of the SNR triggers the switching of the modulation to the next higher order of 8PSK. This process is the same for the rest of the operation. Fig.3, in comparison to fig.2 shows that the algorithm maintains a constant peak BER at varying SNR; QPSK to 128PSK, the algorithm maintains the BER at or below $1x10^{-2}$.

5. Conclusions

An adaptive Haar wavelet-OFDM system has been demonstrated in this work. With this, high power efficiency through link quality management is achieved. For a test, an arbitrary BER number was chosen to test the efficiency of the system. Based on the input test parameters, the BER was successfully kept at a peak BER of $1x10^{-2}$ even at higher constellation orders. In the future, we will extend this work to include the Multiple Input Multiple Output (MIMO) antenna system alongside code rate.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, the project of Science and Technology Department of Chongqing Municipality, Chengdu Chengdian Network Technology Co., Ltd., Chengdu Civil-military Integration Project Management Co., Ltd., and Sichuan Yin Ten Gu Technology Co., Ltd.

References

[1] T. S. Rappaport et al., "Wireless communications and applications above 100 GHz: Opportunities and challenges for 6G and beyond," *IEEE Access*, vol. 7, pp. 78729-78757, 2019.

[2] Ding, Aaron Yi & Janssen, Marijn. (2018). Opportunities for applications using 5G networks: requirements, challenges, and outlook. 27-34. 10.1145/3278161.3278166.

[3] M. A. Tzannes and M. C. Tzannes, "Bit-by-bit channel coding using wavelets," [Conference Record] GLOBECOM '92 - Communications for Global Users: IEEE, Orlando, FL, USA, 1992, pp. 684-688 vol.2.

[4] Sameer A. Dawood, F. Malek, M. S. Anuar, and Suha Q. Hadi, "Discrete multiwavelet critical-sampling transform-based OFDM system over Rayleigh fading channels," Mathematical Problems in Engineering, vol. 2015, Article ID 676217, 10 pages, 2015.

[5] M. Chafii, Y. J. Harbi and A. G. Burr, "Wavelet-OFDM vs. OFDM: Performance comparison," 23rd International Conference on Telecommunications (ICT), Thessaloniki, 2016, pp. 1-5.

[6] Mordecai F. Raji et al, "A new approach for enhancing the services of 5G mobile network and IoT related communication devices using wavelet-OFDM and its applications in healthcare," Scientific Programming, https://doi.org/10.1155/2019/3204695, 2020.

[7] M. Torabi and C. Nerguizian, "Adaptive transmission in spectrum sharing systems with alamouti OSTBC under spatially correlated channels," IEEE Trans. Veh. Technol., vol. 66, no. 4, pp. 3131-3142, Apr. 2017.

[8] B. Umasankar, A. D. S Jayalath and X. Fernando, "Adaptive Performance Improvement of OFDM Radio over Fiber Systems," 2007 International Symposium on Signals, Systems and Electronics, Montreal, QC, 2007, pp. 611-614.

[9] V. Sharma, S. Sergeyev and J.Kaur, "Adaptive 2 x 2 MIMO Employed Wavelet-OFDM-Radio Over Fibre Transmission," IEEE Access, vol. 8, pp. 23336-23345, 2020. doi: 10.1109/ACCESS.2020.2970085.

[10] Y. Wang, W. Liu and L. Fang, "Adaptive Modulation and Coding Technology in 5G System, "2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 2020, pp. 159-164.

WAVELET-BASED COUGH SIGNAL DECOMPOSITION FOR MULTIMODAL CLASSIFICATION

BLESS LORD Y. AGBLEY[1], JIANPING LI[1], AMIN UL HAQ[1], BERNARD COBBINAH[1], DELANYO KULEVOME[2], PRISCILLA A. AGBEFU[3], BRIGHT ELEEZA[4]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 611731-China
[2]School of Information and Communication Engineering, University of Electronic Science and Technology of China Chengdu 611731-China
[3]University of Education, Winneba – Ghana, [4]Koforidua Technical University – Ghana.
E-MAIL: agbleybless@std.uestc.edu.cn, jpli2222@uestc.edu.cn, khan.amin50@yahoo.com, cobbinahbernard@ieee.org, kdelanyo@ieee.org, agbefuabl@gmail.com, brighteleeza1@gmail.com

Abstract:

Signal classifications have benefited from the successes of ML and DNN architectures. Cough classification techniques mainly extract features such as the Mel Frequency Cepstral Coefficients for training. Most of these works also focus on obtaining information from single data modalities. However, multimodal analysis has been shown to aggregate useful information from different modalities thereby improving the internal capacity of ML models at data analysis. In this research, we propose a multimodal cough data classification approach with scalograms images obtained by decomposing cough signals using continuous wavelet transform and clinical information of subjects obtained from the COUGHVID dataset. Our result shows improved precision as compared to expert analysis.

Keywords:

Multimodal analysis; Wavelet transform; Deep learning; Transfer learning

1. Introduction

Deep learning techniques have fueled recent data-driven technologies in diverse sectors including medicine and clinical practices due to their ability to internally identify features and capitalize on patterns and traits from such large datasets. The urgency of finding a solution to the COVID-19 pandemic had resulted in the application of such DL method over data collected on image, sound, and demographic data of patients[1-2]. The use of multimodal data had been shown to be effective at revealing characteristics from the different modalities that could help in recommendation systems or prediction of diseases[3-4].

Signal processing techniques have also been extensively used in medical data analysis to extract useful features from ECG, cough sounds, etc. Wavelet Transform had been particularly researched for its trait of decomposition, denoising and compression of signals[5-6]. In this work, continuous wavelet transform is used to decompose cough signals and the resulting coefficients in form of a scaleogram are used in a multimodal DL training pipeline.

1.1. Organization

The rest of the paper is organized as follows; We state the motivation and some recent works in section 2. Section 3 describes our proposed approach and results. We then gave a conclusion in section 4.

2. Motivation and Related Works

The response by the research community towards obtaining solutions to the COVID-19 pandemic has resulted in a number of proposed techniques based on different datasets collected across the globe. Cough data is one that could be easily collected with most personal mobile devices equipped with microphones. This has enabled institutions to gather data for cough analysis without getting into direct contact with the donor of the data. Orlandic et al released their large-scale crowdsourced dataset named COUGHVID[7] which was motivated by a recent cough analysis paper by Imran et al. [8]. Their paper was based on the hypothesized that that "Cough sounds of COVID-19 patients contain unique enough latent features to be used as a diagnosis medium". They further investigated the uniqueness of COVID-19 cough and found that it was enough to produce a diagnosis based on AI, thus, dissimilar

pathomorphological alternations are present in the respiratory system as a result of COVID-19. They performed their training and testing on their single modal cough sounds dataset of which 96 were bronchitis, 130 were pertussis, 70 were COVID-19, and 247 were normal cough examples collected from different people.

In a much more related work, Brown et al [9] proposed a multimodal machine learning pipeline that utilizes both cough and breath data in their analysis. The authors crowdsourced their respiratory sounds data using the web and an Android App. A total of 141 cough and breathing samples of different COVID-19 patients were used for their final. Over 2200 cough and breath data were also collected from their control group labelled as non-COVID based on different criteria.

In this paper, we show that using the coefficients obtained by decomposing cough signals using continuous wavelet transforms together with some clinical features offers a good prospect for classifying the cough signals. We thus propose a multimodal classification pipeline that takes the decomposed coefficients in form of a scalogram and relevant clinical features from the COUGHVID dataset. These two modalities are passed to a DNN for training and subsequent testing.

3. Methodology

3.1. Dataset and Preprocessing

To the best of our knowledge, as at the time of conducting this research, the largest publicly available cough dataset of COVID-19 patients was the COUGHVID dataset[7]. We opted to use this dataset because of the clinical information provided as metadata. We first filtered the data by removing all records for which no cough was detected. Then as an essential step before performing the decomposition, we trimmed out all the silent parts of the signals.

3.2. Signal Decomposition

Continuous Wavelet Transform analysis is similar to the STFT analysis, but CWT analyzes the cough sound signals in time-frequency. The CWT of 1D sound signals is shown below as:

$$CWT(x,\psi)(s,\tau) = \int_{-\infty}^{+\infty} x(t)\psi^*\left(\frac{t-\tau}{s}\right)dt \qquad (1)$$

The output of CWT coefficients which are functions of scale(s) and time (t).

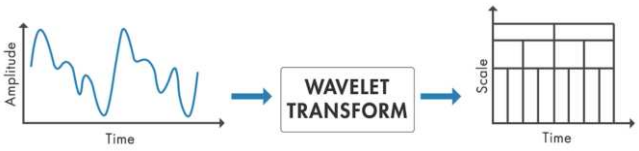


Fig.1 Continuous Wavelet Transform

The 1-D cough signals were decomposed using continuous wavelet transform. The analytic Morlet (Gabor) wavelet was used in the filter banks. Figure.2 shows the original signal, the scalogram of all the coefficients and the signal of the 32nd scale. The Scalograms were obtained using the jet color map. The sampling frequency was kept the same as was used in sampling the cough sounds (48 kHz).

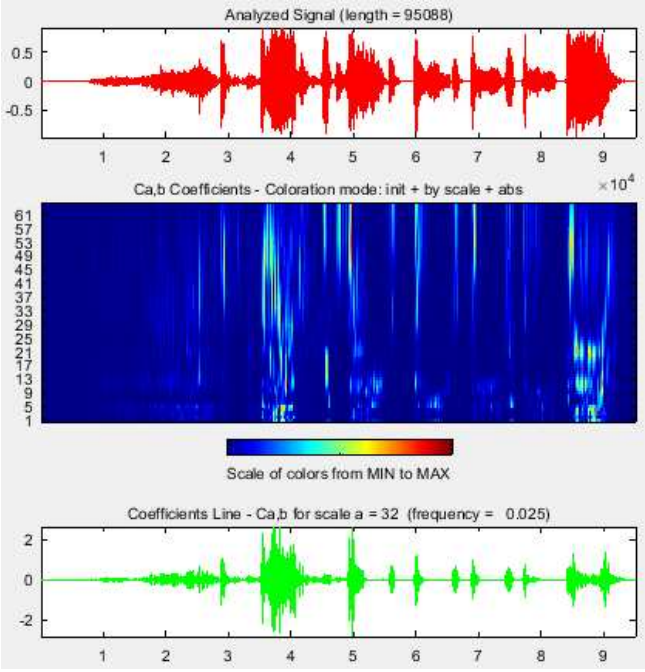


Fig.2 (a) Plot of the original cough signal. (b) Scalogram after decomposing the original signal into 61 scales. (c) A plot of the coefficient of the 32nd scale.

3.3. Transfer Learning

In order to improve the accuracy of our model, we first implemented a transfer learning to learn the initial weights of the image network. This was achieved using autoencoder which usually includes the encoding and decoding processes[10]. Thus, given an input x, the first step is for the autoencoder to encode x to some hidden layers following some encoding processes, after which comes the decoding of the hidden layers to get an output $\hat{x}$. The deviation of $\hat{x}$ from the input x is minimized by the autoencoder.

$$Encoding: \xi = f(W_1 x + b_1) \quad (2)$$

$$Decoding: \hat{x} = f(W_1' \xi + b_1') \quad (3)$$

Where f is a nonlinear activation function, $W_1 \in \mathbb{R}^{k \times m}$ and $W_1' \in \mathbb{R}^{m \times k}$ denote weight matrices. $b_1 \in \mathbb{R}^{k \times 1}$ and $b_1' \in \mathbb{R}^{m \times 1}$ denote bias vectors. The output of the hidden layer is $\xi \in \mathbb{R}^{k \times 1}$. The aim here is to learn some weight matrices and bias vectors that will minimize the reconstruction error:

$$\min_{W_1, b_1, W_1', b_1'} \sum_{i=1}^{n} \|\hat{x} - x\|^2 \quad (4)$$

We use our base CNN architecture for the image as described in the next subsection for the transfer learning. The weights are used to initialize the training of the model.

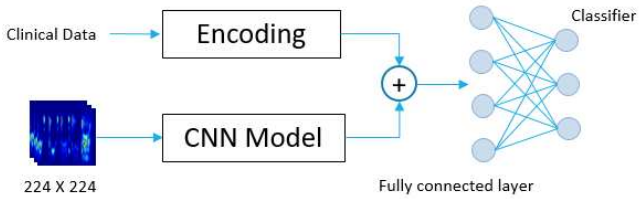


Fig.3 Proposed multimodal architecture

3.4. Fusion-based Classification

From the metadata, we selected and encoded the following features: age, respiratory condition and fever muscle pain, as one modality. These features are first fed into a dense layer with 20 units. The output was then passed into another dense layer with 10 units. ReLU activation layer is used in both layers.

The second modality is the scalogram images. These images were all kept at equal size of 224 × 224 × 3 and fed into the CNN based classifier. The input scalogram images were first passed through two convolutional layers with a filter size of 16 each. The high dimensional output is then sent through a 2 × 2 max-pooling layer thereby reducing the complexity of the model. The next layers are two convolutional blocks with filter sizes of 32 and 64 respectively. Each of the convolutional blocks is made up of two 2-D convolutional layers with a 3 × 3 kernel size, a batch normalization layer and a 2 × 2 max-pooling layer. A dropout of 0.2 is applied to the output features and passed to a fully connected layer. The output features are then passed to a dense block. The dense block is made up of a dense layer with 512 neurons, a batch normalization layer and another dropout of 0.2. The final layer is comprised of a dense layer of 10 neurons.

The features from the two modalities are merged together and fed into a dense layer with 3 neurons and a softmax activation layer for prediction.

3.5. Implementation

The base architecture for the scalogram was used to train a transfer learning on all the images that were not used for either training or test set. To obtain this set, all records for which the cough detection confidence is less than or equal to 0.79 or records where there was no age information were reserved for training the transfer learning model. In addition, 844 records with confidence above 0.79 were also included. A total of 18562 cough sounds were used for the transfer learning. The Training set contains 1116 records of which each class had 372 records. The test set includes 340 records analyzed by experts. Here, the three classes (upper infection, lower infection and obstructive disease) were condensed into a symptomatic class so we can compare the expert accuracy with our model's accuracy. During training, we set our batch size to 16 and used the Adam optimizer with learning rate of 0.0001.

To evaluate our model, we calculated and compared the specificity, sensitivity and precision [11–18] of our model with that of experts' diagnosis over the test set.

$$Specificity = \frac{TN}{TN+FP} \quad (5)$$

$$Sensitivity = \frac{TP}{TP+FN} \quad (6)$$

$$Precision = \frac{TP}{TP+FP} \quad (7)$$

3.6. Results

The results of our proposed model, together with the expert's prediction performance is showed in Table 1.It can be deduced that our model outperformed the experts' diagnosis due to the discriminative feature extraction capability of the deep learning model. Most often, the experts failed to predict the true status of one of the three groups (COVID-19, Healthy and Symptomatic) leading to a very low sensitivity values 0.29, 0.18 and 0.38 respectively.

Table 1 Performance metrics

	Specificity	**Sensitivity**	**Precision**
Experts			
COVID-19	0.78	0.29	0.35
Healthy	0.76	0.18	0.28
Symptomatic	0.49	0.38	0.38
Proposed Model			
COVID-19	0.81	0.43	0.56
Healthy	0.80	0.51	0.58
Symptomatic	0.63	0.69	0.64

4. Conclusion

Cough classifications have mainly been approached using features extracted from Mel Frequency Cepstral Coefficients. In this paper, we show that scalograms obtained by wavelet decomposition could be fused with clinical data for a multimodal classification. COUGHVID crowdsourced public dataset was used for the implementation. To the best of our knowledge, this work is the first to use the dataset for a multimodal classification. We compared our result with that of the experts and had a higher precision. We will explore using discrete wavelet transforms with different wavelet families in further work.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, the project of Science and Technology Department of Chongqing Municipality, Chengdu Chengdian Network Technology Co., Ltd., Chengdu Civil-military Integration Project Management Co., Ltd., and Sichuan Yin Ten Gu Technology Co., Ltd.

References

[1] H. Farhat, G. E. Sakr, and R. Kilany, "Deep learning applications in pulmonary medical imaging: recent updates and insights on COVID-19," Mach. Vis. Appl., vol. 31, no. 6, pp. 1–42, 2020.

[2] M. B. Jamshidi et al., "Artificial Intelligence and COVID-19: Deep Learning Approaches for Diagnosis and Treatment," IEEE Access, vol. 8, pp. 109581–109595, 2020.

[3] K. Chang et al., "Multimodal imaging patterns predict survival in recurrent glioblastoma patients treated with bevacizumab," Neuro. Oncol., vol. 18, no. 12, pp. 1680–1687, Dec. 2016.

[4] D. Zhang and D. Shen, "Multi-modal multi-task learning for joint prediction of multiple regression and classification variables in Alzheimer's disease," Neuroimage, vol. 59, no. 2, pp. 895–907, Jan. 2012.

[5] J. Guan, R. Lai, and A. Xiong, "Wavelet Deep Neural Network for Stripe Noise Removal," IEEE Access, vol. 7, pp. 44544–44554, 2019.

[6] R. K. Srinanthini, P. Srinivasan, and S. Arun, "Spectral Analysis of EEG Data for Ocular Artifact Removal Using Wavelet Transform Technique," in 2019 International Conference on Recent Advances in Energy-efficient Computing and Communication (ICRAECC), 2019, pp. 1–4.

[7] L. Orlandic, T. Teijeiro, and D. Atienza, "The COUGHVID crowdsourcing dataset: A corpus for the study of large-scale cough analysis algorithms," Sep. 2020.

[8] A. Imran et al., "AI4COVID-19: AI Enabled Preliminary Diagnosis for COVID-19 from Cough Samples via an App," Informatics Med. Unlocked, vol. 20, Apr. 2020.

[9] C. Brown et al., "Exploring Automatic Diagnosis of COVID-19 from Crowdsourced Respiratory Sound Data," Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Min., pp. 3474–3484, Jun. 2020.

[10] F. Zhuang, X. Cheng, P. Luo, S. J. Pan, and Q. He, "Supervised representation learning: Transfer learning with deep autoencoders," in IJCAI International Joint Conference on Artificial Intelligence, 2015.

[11] A. Ul Haq, J. Li, M. H. Memon, J. Khan, and S. Ud Din, "A novel integrated diagnosis method for breast cancer detection," J. Intell. Fuzzy Syst., no. Preprint, pp. 1–16, 2020.

[12] A. U. Haq et al., "Feature selection based on L1-norm support vector machine and effective recognition system for Parkinson's disease using voice recordings," IEEE access, vol. 7, pp. 37718–37734, 2019.

[13] A. U. Haq et al., "Comparative analysis of the classification performance of machine learning classifiers and deep neural network classifier for prediction of Parkinson disease," in 2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 2018, pp. 101–106.

[14] A. U. L. HAQ et al., "Identifying the Predictive Capability of Machine Learning Classifiers for Designing Heart Disease Detection System," in 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, 2019, pp. 130–138.

[15] A. U. Haq, J. P. Li, M. H. Memon, S. Nazir, and R. Sun, "A hybrid intelligent system framework for the prediction of heart disease using machine learning algorithms," Mob. Inf. Syst., vol. 2018, 2018.

[16] J. P. Li, A. U. Haq, S. U. Din, J. Khan, A. Khan, and A. Saboor, "Heart Disease Identification Method Using Machine Learning Classification in E-Healthcare," IEEE Access, vol. 8, pp. 107562–107582, 2020.

[17] A. U. Haq, J. Li, M. H. Memon, M. H. Memon, J. Khan, and S. M. Marium, "Heart Disease Prediction System Using Model Of Machine Learning and Sequential Backward Selection Algorithm for Features Selection,"

in 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), 2019, pp. 1–4.
[18] A. Ul Haq et al., “Recognition of the parkinson’s disease using a hybrid feature selection approach,” J. Intell. Fuzzy Syst., no. Preprint, pp. 1–21.

SINGLE IMAGE DEHAZING JOINTLY UTILIZING DARK CHANNEL PRIOR AND GUIDED FILTERING IN DUAL-TREE COMPLEX WAVELET DOMAIN

YUE DONGQIAO[1], HUANG YUANYUAN*[1], TANG HAOZHE[1], HUANG XI[1], QIN ZHI[1]

[1]Department of Network Engineering, Chengdu University of Information Technology, Chengdu, 610225, China
E-MAIL: *hy@cuit.edu.cn

Abstract:

In this paper, a new image haze removal algorithm is proposed by jointly utilizing dark channel prior and guided filtering in dual-tree complex wavelet transform domain. The algorithm firstly uses guided filtering to smooth the hazing image, then adopts dual-tree complex wavelet transform to decompose the hazing image into low-frequency and high-frequency sub-band components, and then uses the dark channel prior model to process the low-frequency sub-band of the image, finally adopts inverse dual-tree complex wavelet transform to get the dehazed image. The dark channel prior comes from the statistical law of the outdoor fog-free image datasets. Since dual-tree complex wavelet transform has approximate translation advantages such as degeneration, higher positioning accuracy, computational efficiency, and guided filtering can increase the scope of application of haze removal, which can greatly reduce the optimization time of initial transmittance and the complexity of the entire algorithm. Therefore, the new proposed algorithm outperforms traditional dark channel prior based defogging algorithm. The experimental results show that the proposed algorithm can effectively improve the contrast and clarity of the image.

Keywords:

Dehaze; Dark channel prior; Guided filtering; Dual-tree complex wavelet transform

1. Introduction

Due to fog or poor air quality, the visibility of the outside scene will reduce and the decrease of the amount of light will cause distortion and lower contrast in the images when shooting some outside scenes. Nowadays, because of the limitations of single image analysis, the processing results of many computer vision technologies such as object detection and image classification are not optimistic. In 2011, He[1] proposed an image defogging algorithm based on the dark channel prior. He found that in a foggy image, some RGB three-channel pixels with at least one low intensity value will be in the atmosphere. When the light rises under the irradiation, these pixels can be repaired to play the role of defogging. In 2013, He [2] proposed guided filtering. On the one hand, this wave filter has good characteristic of maintaining smooth edges, on the other hand, it can make the filter output more structured than the input. By combining the two algorithms, the guided filtering algorithm can compensate for the slower calculation speed of the dark channel prior due to the higher computational complexity [4]. In 2019, Bi [3] proposed that the two-dimensional double-tree complex wavelet's real and imaginary wavelet coefficients can extract high-frequency information in six directions to approximate translation invariance, multi-directional selectivity, higher positioning accuracy and calculation efficiency and other advantages. This paper proposed a new algorithm jointly utilize guided filtering and dark channel prior in dual-tree complex wavelet transform domain. The comparison of experiments under the same conditions shows that the algorithm can effectively improve the image contrast and clarity.

2. Method

2.1. Dark channel prior

In the field of computer vision and computer graphics, McCartney [5] proposed a famous atmospheric scattering model. This model expression is simplified and widely used in the field of image defogging. The expression is as follows:

$$I(x) = J(x)t(x) + A(1-t(x)) \quad (1)$$

Among them, $I(x)$ is the image to be processed (original foggy image), $J(x)$ is the intensity of the scene light and the image we want to get. $t(x)$ is called the transmittance, which reflects the information of the defogging image. A is the atmospheric light intensity. The goal of defogging is to recover J from I. In the algorithm research of He [1], the statistical law of dark channel theory was proposed, which shows that: after decomposing an image into multiple regions, each local region has at least one pixel which has low intensity value on one RGB channel. So the dark channel image is defined according to the following

expression:

$$J^{dark}(x)=\min_{c\in\{r,g,b\}}\left(\min_{y\in\Omega(x)}\left(J^{c}(y)\right)\right) \quad (2)$$

For (1)(2), we then adopt minimum filtering processing to obtain the final expression [5] as shown in the following expression:

$$\tilde{t}=1-\omega\min_{c}\left(\min_{y\in\Omega(x)}\left(\frac{I^{c}(y)}{A^{c}}\right)\right) \quad (3)$$

Among them, the parameter ω is introduced to retain a certain fog effect, so as to play a certain role in the perception of depth of field. If this parameter is removed, the image will be distorted and appear unnatural. The value of ω is 0.95 under normal conditions. Because the transmittance obtained by the dark channel prior algorithm is only a rough transmittance. Need to use soft matting algorithm to refine the transmittance. The optimization problem for t can be approximated by solving the following sparse linear system:

$$(L+\lambda U)t=\lambda\tilde{t} \quad (4)$$

Among them, U is an identity matrix equal to L, and L is the matting Laplacian matrix proposed by Levin, which is usually a parameter value, the purpose of $\tilde{t}$ is to make certain constraints on t. According to the above formula (5) and the a priori law of the dark channel, the atmospheric light value can be used to calculate the final dehazing result. The final result expression is:

$$J_{L}(x)=\frac{I(x)-A}{\max(t(x),t_{0})}+A \quad (5)$$

2.2. Guided filtering

Image filtering is a type of edge smoothing filter, which can realize the functions of image edge smoothing and image fusion denoising. Its principle is to filter the input image through a guide image, and the output image can fully obtain the change details of the guide image while retaining the overall characteristics of the input image [6]. Guided filtering adopts the idea of least squares method, which is calculated by Box Filter and image integration. It has good edge retention and detail enhancement performance. Its execution speed is independent of the filter window size and runs fast. The expression is:

$$q_{i}=\sum_{j}W_{ij}(I)p_{j} \quad (6)$$

In the formula, I is the guide image, and this paper uses the grayscale image of the original image as the guide image; p is the input image; q is the output image; i and j are pixel labels; W_{ij} is the filter kernel function, which is defined as:

$$W_{ij}(I)=\frac{1}{|\omega|^{2}}\sum_{k(i,j)\in\omega_{k}}\left(1+\frac{(I_{i}-\mu_{k})(I_{j}-\mu_{k})}{\sigma_{k}^{2}+\varepsilon}\right) \quad (7)$$

In the formula, ω_{k} is the k-th kernel function window; $|\omega|$ is the number of pixels in the window; μ_{k} and σ^{2} are the mean and variance of the guided image in I the window; ε is the smoothing factor.

2.3. Dual-tree complex wavelet transform

Dual-tree complex wavelet transform (DTCWT) can be realized by applying two pairs of filter banks to the input data at the same time. The complex wavelet can be expressed as:

$$\psi(t)=\psi_{r}(t)+j\psi_{i}(t) \quad (8)$$

In the formula, $\psi_{r}(t)$ represents the real part of the complex wavelet; $\psi_{i}(t)$ represents the imaginary part of the complex wavelet. $\psi_{r}(t)$ and $\psi_{r}(t)$ are real functions. Therefore, DTCWT can be expressed as two independent real wavelet transforms, including two parallel wavelet trees: tree a and b. In order to ensure that the impulse response of the wave filter corresponds to the real and imaginary parts of the complex wavelet transform coefficients, the filter lengths of two trees are used to be odd and even and linear phase respectively. The basic principle is to use a pair of real filter trees to decompose the input signal at the same time to generate the real and imaginary parts of wavelet coefficients.

The two-dimensional dual-tree complex wavelet's real part and imaginary part wavelet coefficients can extract high-frequency information in six directions of $\pm15^{\circ}$, $\pm45^{\circ}$, and $\pm75^{\circ}$. Compared with Discrete Wavelet Transform, it has approximate translation Advantages such as degeneration, higher positioning accuracy and computational efficiency [7]. In contrast, DWT has 3 wavelet sub-bands on each scale, which can only reflect the vertical and diagonal directions of horizontal numbers.

3. Algorithm

After experiments, we found that the image is decomposed into low-frequency and high-frequency parts by dual-number complex wavelet transform. The fogging part caused by the refraction of atmospheric light in the fog component is mainly concentrated in the low-frequency area in the image. After the dual-tree complex wavelet transform, the low-frequency part of the two-dimensional image is subjected to the dark channel prior defogging process, and

the defogging image can be obtained more efficiently. The specific algorithm steps are as follows:

(1) Input a foggy image.

(2) Use guided filtering to obtain the filtered image of the foggy image.

(3) Use the dual-tree complex wavelet transform to obtain the low-frequency and high-frequency components of the input image.

(4) Use the dark channel prior model to process the low-frequency sub-band image.

(5) Adopt inverse dual-tree complex wavelet transform on the new low-frequency sub-band and the old high-frequency sub-band to reconstruct the image.

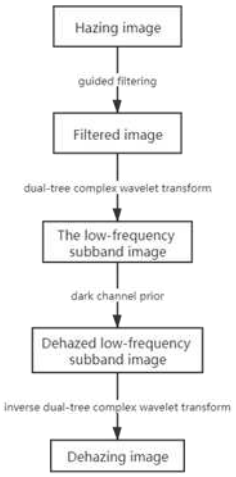


Fig.1 Algorithm flow chart

4. Experimental results and analysis

Compared with the traditional single dark channel prior model, the dual-tree complex wavelet transform combined with guided filtering in dark channel prior domain performs better, because only the extracted low frequency sub-bands need to be processed accordingly. This algorithm can greatly reduce the algorithm time complexity. In order to qualitatively and quantitatively evaluate the results of the image, the results of the dark channel prior algorithm and the result of the dark channel prior image dehazing combined with guided filtering are obtained in the experiment. The contrast and information entropy of the dehazing image are compared in the experiment, as shown in Table 1 below. It can be seen from the table that the algorithm proposed in this paper has increased information entropy and contrast compared with the dark channel prior dehazing algorithm. From the visual observation, the defogging image obtained by this algorithm is obviously higher than the defogging image obtained by the defogging algorithm of other models.

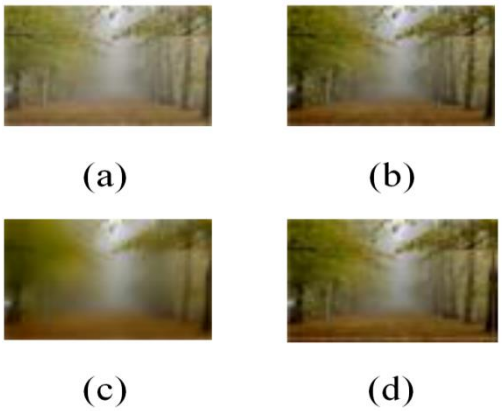


Fig.2 Comparison of woods with fog, (a) Hazing Image, (b) He's method, (c) Guided Filtering with Dark Channel Prior, (d) Our method

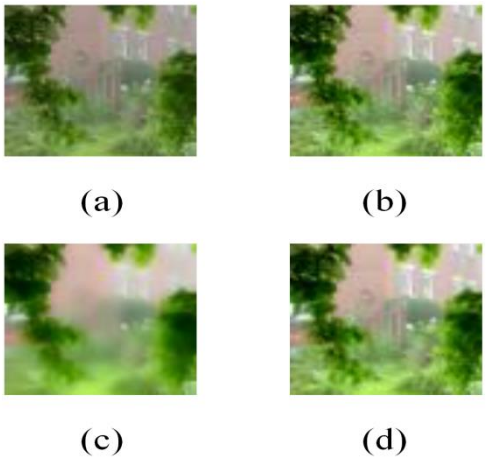


Fig.3 Comparison of a garden with fog, (a) Hazing Image, (b) He's method, (c) Guided Filtering with Dark Channel Prior, (d) Our method

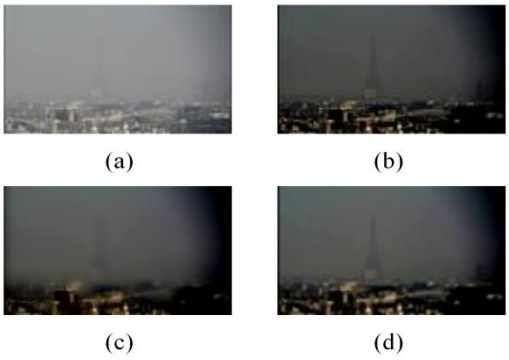


Fig.4 Comparison of a foggy night city, (a) Hazing Image, (b) He's method, (c) Guided Filtering with Dark Channel Prior, (d) Our method

Tablet 1 Comparison of experimental data

Input Image	Algorithm	Entropy	Contrast
1	Hazing Image	7.1956	27.9123
	Method 1	7.4020	34.5871
	Method 2	7.3559	35.4176
	Our method	7.4425	35.8256
2	Hazing Image	7.4136	37.6414
	Method 1	7.6511	50.1367
	Method 2	7.5266	52.3939
	Our method	7.7205	55.6892
3	Hazing Image	5.7625	21.2878
	Method 1	6.0900	29.7418
	Method 2	6.0469	33.9129
	Our method	6.7755	50.8667

5. Conclusions

The algorithm that combines the dark channel prior model proposed in this paper, after introducing the dual-tree complex wavelet transform and guided filtering, indeed effectively improves the efficiency of the algorithm. In addition, since the algorithm only dehzed the low-frequency sub-band components, the next step will consider improving the high-frequency components of the image. Moreover, because the dark channel prior is a statistical law, it may not be effective for some very special images. For example, when the scene is essentially close to the air layer and there is no shadow covering it, the dark channel theory is Invalid.

Acknowledgements

This paper is supported in part by Sichuan Science and Technology Program under Grants 2018RZ0072 and 20ZDYF0660, in part by 2018 China Meteorological Administration Soft Science Independent Project under Grant 09, in part by Foundation of Chengdu University of Information Technology under Grant J201707, in part by College Students' innovation project of Chengdu University of Information Technology under Grants S201910621082, 202010621260 and 202010621268.

References

[1] Kai-ming, He, Jian, Sun, Xiao-ou, Tang. Author, “Single image haze removal using dark channel prior”, IEEE transactions on pattern analysis and machine intelligence, pp. 2341-53, 2011.

[2] Kai-ming, He, Jian, Sun, Xiao-ou, Tang. Author, “Guided Image Filtering”, in IEEE Transactions on Pattern Analysis and Machine Intelligence, pp. 1397-1409, June 2013.

[3] Siwen B I , Hao C , Tong S , et al. Author, “An Image Denoising Algorithm Based on Double-tree Complex Wavelet Transform”, Radio Engineering, pp, 2019.

[4] QIN Hong-chao, LI Yan-yan, LONG Wei, et al. Author, “Real- time video dehazing based on dark channel prior”, Computer Engineering and Applications, pp. 176-181, 2018.

[5] E. J. McCartne1y. Author, “Optics of Atmosphere: Scattering by Molecules and Particles”, New York : John Wiley and Sons , pp. 23-32, 1976.

[6] TANG Jian-bo,JIANG Tie, WANG Tian. Author, “Research on Single Image Dehazing Using Guided Filtering”, Science Technology and Engineering, pp. 3021-3025+3042, 2013.

[7] Huang Xue-you, Zhang Chang-jiang. Author, “MRI denoising based on dual-tree complex wavelet transform”, Journal of Image and Graphics, pp. 104-113, 2016.

OPTIMIZATION OF LAPLACE WAVELET DICTIONARY FOR SPARSE DECOMPOSITION OF EARLY WEAK SIGNAL OF ROLLING BEARING BASED ON ARTIFICIAL BEE COLONY ALGORITHM

ZHANG SHUO[1], LI FUSHENG[2]

[1, 2]School of Automation Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
E-MAIL: zhangshuo951227@hotmail.com, lifusheng@uestc.edu.cn

Abstract:

The transient components in the early weak fault vibration signals of rolling bearings are easily obscured by intense background noise and cannot be detected quickly. Based on the sparse representation principle, an artificial bee colony (ABC) optimization sparsity method of the Laplace wavelet dictionary is proposed to realize the transient characteristic components in the signal extraction. Sparse decomposition with Orthogonal Matching Pursuit (OMP) algorithm is a signal adaptive decomposition algorithm, and it is one of the effective methods for weak feature extraction under strong noise background. Aiming to select and construct an over-complete dictionary for the sparse representation of rolling bearing fault vibration signals, based on the analysis of fault signals' characteristics, an improved Laplace wavelet atomic library was constructed. For solving extensive calculation and low efficiency of the orthogonal matching pursuit algorithm, this paper combines the ABC algorithm's fast operation characteristics to select the improved Laplace wavelet atom that best matches the fault through the inner product operation, thereby improving the calculation efficiency. Experiments show that the method has a proper matching with the early weak fault signals of rolling bearings and can adequately characterize fault information and judge the fault type more accurately.

Keywords:

Fault diagnosis; Improved Laplace wavelet; Sparse decomposition; Artificial bee colony algorithm; Rolling bearing

1. Introduction

As an essential part of the mechanical system components, rolling bearings often fail during the automatic system operation. Once the failure occurs, it will have a considerable impact on the normal functioning of the equipment. Therefore, it is incredibly essential to perform condition monitoring and early fault diagnosis on rolling bearings to ensure the material's safe operation in the later stages. Rolling bearings are subject to pitting, spalling, and other failures[1-3]. The existence of these failures will cause periodic impulse vibration. The basic waveform is a combination of a sine wave and an impulse attenuation response waveform. Its characteristic frequency depends on the fault location, speed, and bearing parameters; this coexistence of different typical waveforms brings specific difficulties to bearing fault feature extraction and failure location diagnosis [4-6].

Unlike traditional signal characterization methods, the signal sparse characterization theory aims to find the sparsest expression from the redundant basis function library and then realizes the capture of the essence of information and the most efficient illustration. The specific components of mechanical faults often show sparseness in the overall signal. Suppose the sparsest representation of the original message based on a particular feature dictionary can be found, and a matching dictionary with signal fault characteristics can be selectively constructed. In that case, the dictionary selection and update can be more matchable to the original signal structure. Built on the time-frequency theory, Mallat et al.[7]proposed a Gabor atomic library. The local aggregation of Gabor atoms in the time-frequency domain conducts well, which can adequately represent the signal's regional characteristics. Still, because Gabor atoms' frequency does not change with time, it is sometimes difficult to match some typical FM signals [8].In 1999, Buttlan et al.[9] proposed that Chirplet atoms were constructed by adding chirp parameters based on Gabor atoms, and the Chirplet frequency changed linearly with time. There was a certain degree of distortion in matching bearing fault signals. Xiaohui Gu et al.[10]formed a Laplace wavelet. The single attenuation characteristic of the wavelet base effectively matches the fault signal, but the lack of orthogonality limits its application. Aiming at this problem, the improved Laplace wavelet is introduced to represent bearing fault signals sparsely. The main algorithm of traditional atomic search is the matching pursuit (MP) search method, which approximates the original signal of the optimal local value found in each iteration. Take into account this, the orthogonal

matching pursuit algorithm (OMP) is developed. Although this method has high accuracy, the calculation effectiveness is low, and the real-time performance is not superior. Owing to the relative efficiency of smart algorithms in optimization, intelligent algorithms can significantly improve search efficiency. Therefore, to speed up the ability of the atomic search, Yousef Zanjireh et al.[11] proposed an optimization algorithm for selecting dictionary atoms based on genetic calculations, but this algorithm has a slower search speed and quickly falls into a local optimum.

Aiming at the above problems, this paper proposes a signal sparse decomposition method based on the ABC algorithm to optimize the Laplace wavelet dictionary. First, the signal is sparsely decomposed using the improved Laplace wavelet atoms. The optimized OMP algorithm is utilized to perform atomic optimization, and then the reconstructed signal is extracted. Sensitive features are used as feature parameters and applied to the analysis of rolling bearing fault simulation and measured signals.

The rest of this article is organized as follows. The second part introduces the methods and related background theories proposed in this paper. The third part analyzes the simulation signals and compares them with other methods (GA-OMP). In Section Four, the experimental verification and engineering applications are performed, which solves detecting the rolling bearing's early weak fault. Finally, Section five concludes.

2. Optimization of Laplace wavelet dictionary based on ABC algorithm

2.1. Improved Laplace wavelet dictionary

The frequency component of a rolling bearing signal often changes over time due to bearing defects and faults. When the bearing surface is damaged, periodic waveforms and impulsive attenuation waveforms often appear in the collected vibration signals. To further improve the matching performance of time-frequency atoms to nonlinear FM signals, Laplace wavelet atoms are used to build a sparse dictionary:

$$g_r = A \times e^{2\pi ft \frac{-\xi}{\sqrt{1-\xi^2}}} \times \sin 2\pi ft \qquad (1)$$

Atomic parameter set $\gamma = (f, \zeta)$, where A, f, ξ are the coefficients of normalized wavelet functions, oscillation frequency, and Damping coefficient, respectively.

The Laplace wavelet and impact signals' correlation coefficient is high, while the Laplace wavelet and noise and other signals are low. Finding an appropriate Laplace wavelet can accurately identify impact signals. Atoms are applied to the analysis of bearing fault signals. To obtain an over-complete dictionary with high redundancy, its time-frequency parameters need to be discretized by the optimization algorithm.

2.2. Principle of the improved OMP algorithm

This paper optimizes the OMP algorithm by the ABC algorithm. Secondly, the ABC_OMP algorithm is tuned by changing the residual update's timing to accelerate the speed of signal decomposition. $\mathbf{D} = \{\mathbf{g}_\gamma(\mathbf{t})\}_{\gamma \in \Gamma} (\Gamma = \{\gamma_i, i = 1, 2, ...\})$ is a group of an over-complete dictionary of Hilbert space H, $\mathbf{g}_\gamma$ is a dictionary atom defined by parameter group γ, and this atom is standardized, e.g., $\|\mathbf{g}_\gamma\| = 1$. f is a signal to be analyzed. The process of ABC_OMP is as follows:

Step 1: Input signal to be decomposed f. OMP algorithm initialization, set the number of iterations, let $k = 0$.

Step 2: Initialization of ABC algorithm, search times limit, and the maximum number of loop iterations max. Randomly generated N initial viable atoms, corresponding to the hired bee;

Step 3: Calculate the fitness function value of the corresponding atom of the hired bee, and record the optimal atomic parameter vector γ^* and the maximum fitness function value $fitness(\gamma^*)$; According to the formula $\mathbf{v_{kj}} = \gamma_{\mathbf{kj}} + R_{kj}(\gamma_{\mathbf{ij}} - \gamma_{\mathbf{kj}})$, the hired bee performs a neighborhood search and calculate the fitness function value of the corresponding new atom (The parameter vector is $\mathbf{v_k}$), if $fitness(\mathbf{v_k}) > fitness(\gamma_{\mathbf{k}})$, then $\gamma_{\mathbf{k}} = \mathbf{v_k}$, or $\gamma_{\mathbf{k}}$ is constant. And update the optimal atomic parameter vector γ^* at the same time and the maximum fitness function value $fitness(\gamma^*)$;

Step 4: The waiting bee chooses the atom randomly, and perform a neighborhood search to generate new atoms according to the formula $\mathbf{v_{kj}} = \gamma_{\mathbf{kj}} + R_{kj}(\gamma_{\mathbf{ij}} - \gamma_{\mathbf{kj}})$, the parameter vector is $\mathbf{v_k}$, and calculate the fitness function value for the new atom. Hiring bees through a limit cycle determine whether the corresponding initial atom is updated. If the kth atom is not updated, the hired bee turns into a scout bee and generate a new atom (the parameter vector is $\mathbf{r_k}$).

Step 5: repeat step 3~step 4, up to the maximum number of iterations max. Save the optimal atomic parameter vector at this time $\gamma_{\mathbf{k}}^* = \gamma^*$ and the maximum fitness function value $fitness(\gamma_{\mathbf{k}}^*) = fitness(\gamma^*)$.

Fig.1 is a flowchart based on improved OMP.

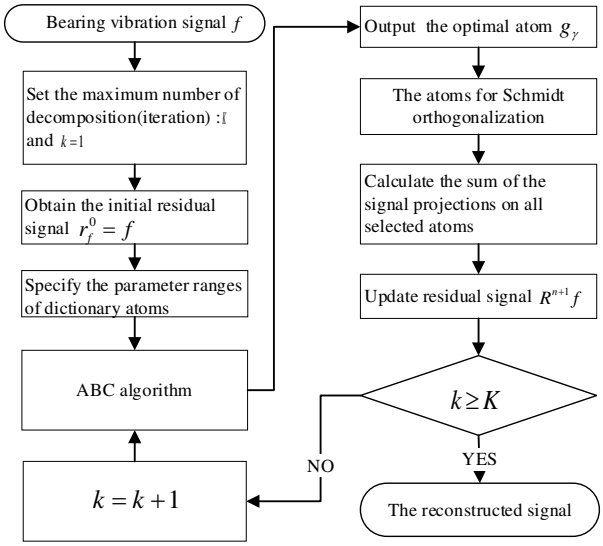


Fig.1 Flow chart of the proposed method

3. Results and analysis

This section evaluates the proposed method's effectiveness and analyzes the bearing outer ring fault signal as a simulation signal. For a faulted bearing with a partial outer ring defect, the following formula is used to simulate its vibration signal:

$$y(t) = y_0 e^{-\zeta\omega_n t} \sin \omega_n \sqrt{1-\xi^2}\, t \tag{2}$$

where y_0 and ζ are scale factor and damping coefficient, respectively, $\omega_n = 2\pi f_n$, f_n is the normal operating frequency of the bearing. Let y_0, ζ , f_n be 5, 0.1, 3000Hz, impact repetition cycle is 0.01s. The sampling frequency of the signal is 20kHz; the number of sampling points is 4096. Add Gaussian white noise to the simulated signal (the noise intensity $d = 0.6$), as Fig.2 (a), (b), and (c) show.

This paper uses Laplace wavelet atoms for sparse decomposition. The atom formula is:

$$g_\gamma = \begin{cases} A \times e^{2\pi f t \frac{-\xi}{\sqrt{1-\xi^2}}} \times \sin 2\pi f t, & t \geq 0 \\ 0, & t < 0 \end{cases} \tag{3}$$

The atomic parameter set is $\gamma = (f, \zeta)$, and the parameter range is set as follows: $f \in [1000, 5000]$, $\zeta \in [0.01, 0.3]$. To evaluate the advantages of the proposed method, the comparison is also made in this paper by analyzing the sparse decomposition using traditional genetic algorithms. The maximum number of genetic algorithm and the ABC algorithm and the number of individuals is 200 and 1000. The maximum number of sparse decompositions is 90.

Fig.3 (a), (b), 4 (a), and (b) show the reconstructed and residual signals obtained by the two methods, respectively.

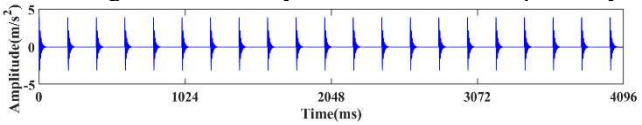


Fig.2(a) Simulation signal

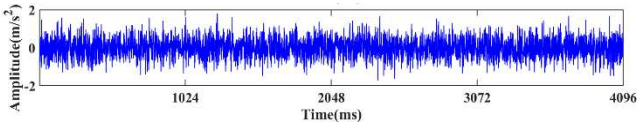


Fig.2(b) The Gaussian white noise signal

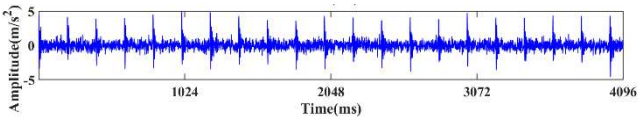


Fig.2(c) Synthesized signal of simulated signal and noise signal

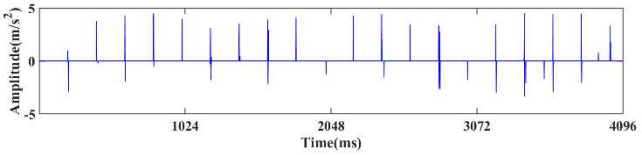


Fig.3(a) Signal reconstructed using genetic algorithm

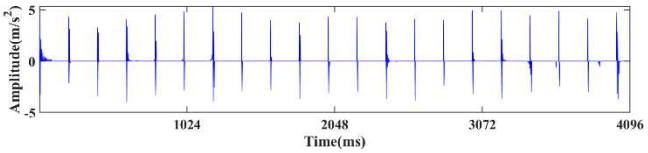


Fig.3(b). Signal reconstructed using ABC algorithm

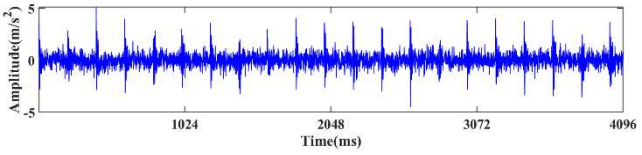


Fig.4(a). Residual signal using the genetic algorithm

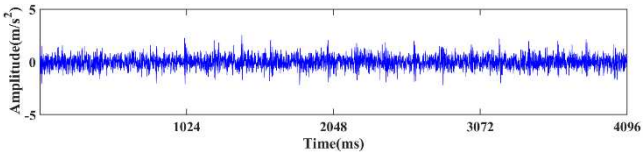


Fig.4(b). Residual signal using the ABC algorithm

Table 1 Comparison of parameters in simulation results

Method	ABC-OMP	GA-OMP
The correlation coefficient	0.67	0.42
SNR(dB)	-2.695	-5.442
Residual signal energy(m/s^2)	1363	2155

For simulation signals with white Gaussian noise, both can reconstruct the signal. Still, the proposed method has higher reconstruction accuracy and could effectively reconstruct valid signals in the same number of reconstructions. The remaining signals are mostly noise signals. Simultaneously, due to the advantages of the involved Laplace wavelet atomic dictionary, the proposed dictionary OMP has excellent advantages in mixed-signal reconstruction. Through the above analysis and comparison, the effectiveness and superiority of the technique are proved. This method can reconstruct the bearing fault signal well, which shows that the method can still effectively extract bearing fault characteristics even when the bearing fault signal contains inevitable component noise.

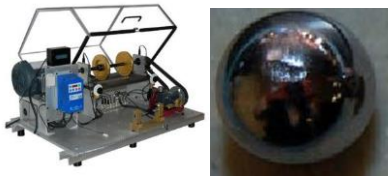


Fig.5 The bevel gear and rolling element bearing failure test bench

Fig.6 Fault bearing rolling element

In this section, the bearing fault vibration signal is based on the data obtained from the bevel gear and rolling bearing failure experiments of the University of Electronic Science and Technology of China. Fig.5 shows the experimental system, including the motor, coupling, rotor, eight-channel data collector, acceleration sensor, speed sensor, bevel gearbox, load, bearing (rolling and sliding) bevel gear, and faulty rolling body is presented in Fig.6. The test bearing model is rolling bearing ER-16K. Table 2 illustrates the specifications. The vibration signal is acquired at a rotation frequency of 30 Hz. The vibration signal is obtained by a data collector mounted on the motor drive side's bearing housing. The sampling frequency is 20kHz, the data point N1 is 4096, and the analysis is performed on a laptop. According to the rotation frequency f_r and bearing specifications, the tested bearing's characteristic fault frequency is calculated.

Table 2 Parameter table of faulty bearing components

Parameters	Value
Ball diameter (inch)	0.3125
Pitch circle diameter (inch)	1.318
Contact angle (°)	0
Number of balls	9

Table 3 Measured bearing fault characteristic frequency

Fault type	Frequency (Hz)
Inner race fault	167.0087
Outer race fault	102.9913
Cage fault	11.4435
Ball fault	59.7075

Fig.7 (a) and Fig.7 (b) show the time-domain and frequency-domain waveforms of the original vibration signals of the tested bearings. It can be seen from the figure that the signal-to-noise ratio (SNR) of the vibration signal is meager, so it is difficult to find its periodic impact part in the time domain waveform. Although the fault characteristic frequency can be observed, the characteristic fault signals are almost entirely submerged in many interference signals, which affects the accuracy and efficiency of fault diagnosis.

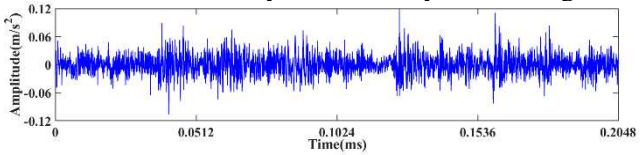


Fig.7(a) Time-domain diagram of a 4096-point bearing outer ring fault vibration signal

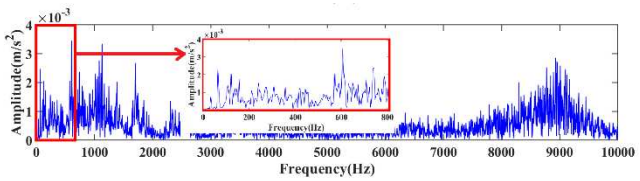


Fig.7(b) Frequency domain diagram of a 4096-point bearing outer ring fault vibration signal

Next, the method proposed in this paper is used to analyze bearing vibration signals. The time-domain waveform, residual signal waveform, and envelope spectrum of the reconstructed signal are shown in Fig.8 (a), Fig.8 (b), and Fig.8 (c).

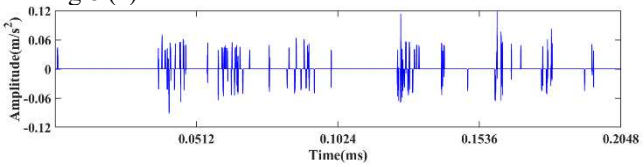


Fig.8(a) Sparse reconstructed signal obtained by the method in this paper

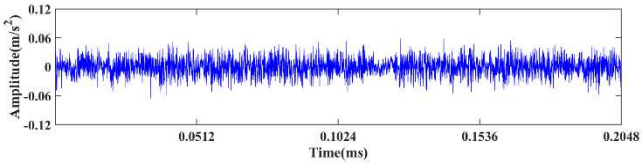


Fig.8(b) Residual signal after sparse reconstruction obtained by the method in this paper

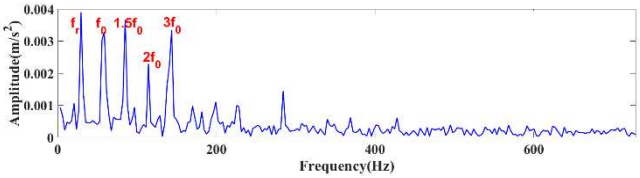


Fig.8(c) Envelope demodulation spectrum of the reconstructed signal

The impact component can be observed in the figure, and the amplitude of the remaining signal is limited to 0.6 to obtain a reconstructed signal with a high signal-to-noise ratio, and the fault frequency can be found through the envelope spectrum (f_0=58.59 Hz). Besides, the harmonics of the characteristic frequency of the fault can be observed from the envelope spectrum of the reconstructed signal (for example $2f_0$=117 Hz , $3f_0$, $1.5f_0$). Nevertheless, we cannot find $3f_0$, $1.5f_0$ in the spectrum of the original signal. The fault diagnosis results are almost the same as the value in Table 3 of the real experiment. The process in this paper has a superior performance.

4. Conclusion

The improved Laplace wavelet dictionary under the OMP framework optimized by the ABC algorithm is applied to bearing fault diagnosis. First, a novel and effective optimization algorithm namely ABC algorithm is introduced. This method is applied to the OMP framework to optimize the atomic parameters and then use the atoms in the atomic library to best match the original signal. Secondly, by analyzing the bearing fault simulation signals and comparing them with those obtained by optimizing the atomic parameters through the traditional genetic algorithm, we can know the proposed method's effectiveness and authority. The main conclusions are summarized as follows:

(Ⅰ) The proposed ABC optimization algorithm based on OMP can better select the atoms which fit the fault signal. Simulation and experimental cases can well prove.

(Ⅱ) Compared with other schemes, the one proposed in this paper shows a better ability to extract bearing fault characteristics, so it has absolute practical value in bearing fault diagnosis.

References

[1] Z. Hua, J. Shi, Y. Luo, W. Huang, J. Wang, and Z. Zhu, "Iterative matching synchrosqueezing transform and application to rotating machinery fault diagnosis under nonstationary conditions," *Measurement*, p. 108592, 2020, doi: https://doi.org/10.1016/j.measurement.2020.108592.

[2] J. Yao, J. Zhao, Y. Deng, and R. Langari, "Weak Fault Feature Extraction of Rotating Machinery Based on Double-Window Spectrum Fusion Enhancement," IEEE Trans. Instrum. Meas., vol. 69, no. 4, pp. 1029–1040, 2020, doi: 10.1109/TIM.2019.2910920.

[3] P. Liang, C. Deng, J. Wu, and Z. Yang, "Intelligent fault diagnosis of rotating machinery via wavelet transform, generative adversarial nets and convolutional neural network," Measurement, vol. 159, p. 107768, 2020, doi: https://doi.org/10.1016/j.measurement.2020.107768.

[4] X. Zhang, Z. Liu, L. Wang, J. Zhang, and W. Han, "Bearing fault diagnosis based on sparse representations using an improved OMP with adaptive Gabor sub-dictionaries," ISA Trans., 2020, doi: https://doi.org/10.1016/j.isatra.2020.07.004.

[5] R.-B. Sun, Z.-B. Yang, Z. Zhai, and X.-F. Chen, "Sparse representation based on parametric impulsive dictionary design for bearing fault diagnosis," Mech. Syst. Signal Process., vol. 122, pp. 737–753, 2019, doi: https://doi.org/10.1016/j.ymssp.2018.12.054.

[6] L. Wang, Z. Liu, H. Cao, and X. Zhang, "Subband averaging kurtogram with dual-tree complex wavelet packet transform for rotating machinery fault diagnosis," Mech. Syst. Signal Process., vol. 142, p. 106755, 2020, doi: https://doi.org/10.1016/j.ymssp.2020.106755.

[7] S. G. Mallat and Z. Zhang, "Matching pursuits with time-frequency dictionaries," IEEE Trans. Signal Process., vol. 41, no. 12, pp. 3397–3415, 1993, doi: 10.1109/78.258082.

[8] T. W. Lun and N. Yahya, "Quad Flat No-Lead (QFN) device faulty detection using Gabor wavelets," in 2015 International Conference on Smart Sensors and Application (ICSSA), 2015, pp. 139–143, doi: 10.1109/ICSSA.2015.7322526.

[9] A. Bultan, "A four-parameter atomic decomposition of chirplets," IEEE Trans. Signal Process., vol. 47, no. 3, pp. 731–745, 1999, doi: 10.1109/78.747779.

[10] X. Gu, S. Yang, and Y. Liu, "Multi-objective Optimized Anti-symmetric Real Laplace Wavelet Filter for Bearing Fault Diagnosis," in 2017 International Conference on Sensing, Diagnostics, Prognostics, and Control (SDPC), 2017, pp. 651–654, doi: 10.1109/SDPC.2017.128.

[11] Y. Zanjireh, A. H. Rezaie, and H. Amindavar, "Multi component signal decomposition based on chirplet pursuit and genetic algorithms," Appl. Acoust., vol. 74, no. 12, pp. 1333–1342, 2013, doi: https://doi.org/10.1016/j.apacoust.2013.05.007.

INVESTIGATION OF HIGH DYNAMIC RANGE IMAGE REGISTRATION ALGORITHM

WANG QINGSONG[1], LI JIANPING[1]

[1] Univ Elect Sci & Technol China, Sch Comp Sci & Engn, Chengdu 611731, Peoples R China
E-MAIL: pineisme@126.com, jpl2222@uestc.edu.cn

Abstract:

Dynamic imaging technology has a wide range of applications. High dynamic image (HDR) can obtain better realism and has irreplaceable advantages over traditional image. Compared with the hardware implementation, the software algorithm using multiple photos with different exposures has the advantages of simpler and lower cost. However, multiple images are prone to different degrees of displacement, which requires image registration technology for image registration. The main contents of this paper are image registration related technology, image synthesis, camera response function fitting, color synthesis and so on. The core problem is to study image registration technology, including mean binarization (MTB). This is an important link in the process of HDR image synthesis and has important practical significance.

Keywords:

Tracking; HDR; MTB; SIFT; Multi-exposure

1. Introduction

Dynamic range refers to the ratio between the maximum pixel value and the minimum pixel value in an image. The traditional digital image can only store the brightness level of a pixel with 8bit (255 level) or 16bit (65536 level), which is called low dynamic range (LDR) Imagine that the white clouds and the midday sun in the low dynamic range images are pure white, but their brightness difference is huge, which is far from being able to be distinguished by hundreds or tens of thousands of levels. Therefore, the traditional LDR digital image cannot restore the real world. With the development of technology, the emergence of high dynamic range (HDR) image solves this problem very well. It uses floating-point number to represent each pixel value, and it is linearly proportional to the actual brightness of the real world, which can better represent the optical characteristics of the real world.

The cost of high dynamic range image obtained by upgrading the hardware is very high, which is not suitable for promotion to ordinary consumers. Therefore, we need software imaging method to obtain high dynamic range image under lower hardware requirements. High dynamic range image synthesis technology emerges as the times require.

In the next few chapters will describe several commonly used images processing methods, using different methods to get a high dynamic range image. And trying to noise the best method.

2. MTB Algorithm

A fast registration algorithm MTB based on pixel value was proposed in Greg Ward's paper [1]. Median threshold Bitmap (MTB) is a widely used and simple algorithm. To obtain the image offset, the most direct method is to compare the edge-based contours of different images. However, the general edge binarization algorithm is not stable enough for images with different exposures, so an MTB algorithm uses the mean binarization algorithm. The first is to get the binarized image.

2.1. Get MTB Image

To get the MTB image, you must first determine the average value of the image pixels, and then set the pixels larger than the average value in the original image to 255, and the pixels smaller than the average value to 0. The pixel average value can be calculated by grayscale Picture pixel histogram, take the median value M.

$$V_1 = \begin{cases} 0, & V < M \\ 1, & V \geq M \end{cases} \quad (1)$$

The value V_i is the pixels of the image that it processed by the MTB algorithm. V is the pixel value of the original image? If it is a color image, it should be converted to a grayscale image. Not only should it be converted to a grayscale image in the mean binarization algorithm, it should be converted to a grayscale image in all subsequent algorithm summaries. First convert the picture to grayscale, because those algorithms can only handle grayscale images.

The RGB image can be converted into a single-channel grayscale image by the following formula:

$$\text{grey} = \frac{(54\times\text{red}+183\times\text{green}+19\times\text{blue})}{256} \quad (2)$$

The picture should only have two kind of pixel value 0 and 255 at the 8-bit situation.

The edge binarization method is usually used for comparison with MTB. So, we apply the MTB method and the edge binarization method to two pictures with different exposures will get different effects (Fig 2).

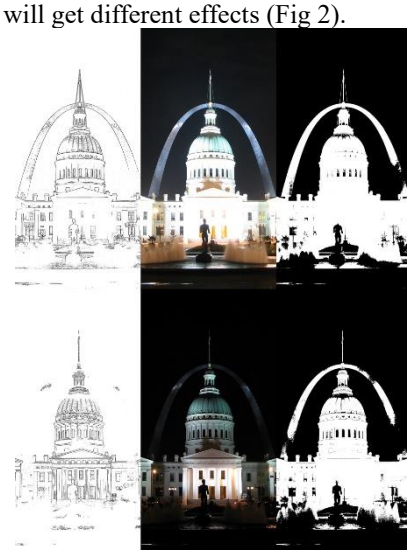


Fig.1 In the middle are two images with different exposures, the left is the image after edge binarization, and the right is the image after median binarization.

Edge binarization will get the edge information of the objects in the image. We used two different MTB methods, one of which got the contour of the image, and the other without contour. Through comparison, it can be seen that the median binarization (MTB) algorithm is more stable than edge binarization, which is beneficial to improve the accuracy of registration. We can see that the MTB method obtain more information about the picture, however, both of these methods have a disadvantage that there is obvious noise, but MTB is obviously better. which is obviously unfavorable for the subsequent processing?

In order to solve the noise problem, we can give the median value a left and right range, for example, in this work the range is 4. We can set the pixel value as this formula:

$$V_2 = \begin{cases} 0, & |V-M| \le 4 \\ V_1, & |V-M| > 4 \end{cases} \quad (3)$$

After the MTB image is obtained, the offset of the two needs to be obtained. This requires the XOR operation of the two MTB images to obtain the difference between the two. The error amount is the number of 1 after the XOR. If you want to get the specific cheap quantity, you can use the brute force search method to search in the XY direction to get the Δx and Δy that minimize the error after the exclusive OR.

$$\text{error} = \sum_{allpixel} XOR(image1, image2) \quad (4)$$

However, for high resolution images, if the above method is used to directly perform translation comparison, it will consume very high time, and an alternative method is needed. In his paper, Ward proposed to decompose each MTB image in multi-resolution, and perform a small-scale brute force search at a low scale, that is, to build an image pyramid, which greatly speeds up the search.

If there is a rotation angle between the images, the offset between the images cannot be completely described accurately, which will affect the synthesis of HDR images. Therefore, in order to make the MTB method more applicable, we have to study the rotation How to get the offset in the rotation angle under the circumstances.

After obtaining the relative translation offset of the image, we need to keep the common part of the binary image of the first two top-level images, and obtain a new pair of images. The center pixel of the two images is taken as the center of the circle, and the image. The smaller value of the length and width is used as the diameter, and the minimum value of the search error for the pixels on the circumference at a certain angle is similar to the translation registration method. Every time the image to be registered is rotated by one pixel, it is performed with the reference image. The XOR operation is summed to find the smallest value among all sums, which is the best matching position. After obtaining the corner offset, the image is registered, and the two images are cropped, and their common part is retained as the final matching position. Accurate results.

If the rotation angle deviation between the images is too large, it may cause a translation and deflection registration to be inaccurate. Therefore, the above translation and deflection operations can be repeated, namely 'translation'->'rotation'->'translation'->'rotation', until the rotation angle offset is 0.

3. Registration algorithm based on SIFT features

SIFT (scale-invariant feature transform) is an image key point (or interest point) detection method proposed by UBC professor David Lowe in 1999 and perfected in 2004 [2], and the key point Local scale invariant features are depicted. A paper published on WSCG2007 by A. Tomaszewski et al. [3] proposed a multi-exposure image registration algorithm based on SIFT features. SIFT feature points are widely used in image recognition and registration. The SIFT feature points can be used to easily match related points on two

images. The SIFT algorithm is an algorithm for extracting local features. The key technical point is the extraction of SIFT feature points. It is necessary to find the extreme points of the image scale space and extract their position, scale, and direction information.

3.1. The feature of SIFT

- The SIFT feature is a local feature of the image, which keeps its rotation, scale scaling, and brightness changes invariant, and it also maintains a certain degree of stability against viewing angle transformation, affine transformation, and noise.
- Uniqueness number, rich in information, used for faster matching in a large amount of data.
- Multi-quantity, seemingly simple objects can also generate a large number of SIFT feature vectors.
- High speed, the optimized SIFT matching algorithm has a faster calculation speed.
- Scalability, SIFT features can be easily combined with other forms of feature vectors.

3.2. Extremum point detection in scale space

To use SIFT to extract potential points of interest, the scale space of the image should first be constructed. Two-dimensional scale space of the image $\mathrm{I}(\mathrm{x},\mathrm{y})$ at different scales is expressed as, $\mathrm{L}(\mathrm{x},\mathrm{y},\sigma)$, Gaussian blur is performed by the image $\mathrm{I}(\mathrm{x},\mathrm{y})$.

$$\mathrm{L}(\mathrm{x},\mathrm{y},\sigma) = \mathrm{G}(\mathrm{x},\mathrm{y},\sigma) * \mathrm{I}(\mathrm{x},\mathrm{y}) \quad (5)$$

Convolution with a two-dimensional Gaussian function to get.

$$\mathrm{G}(\mathrm{x},\mathrm{y},\sigma) = \frac{1}{2\pi\sigma^2} e^{-\frac{(x^2+y^2)}{2\sigma^2}} \quad (6)$$

We perform Gaussian blurring by choosing different standard deviations σ, we make $\mathrm{t} = \sigma^2$, at this time our two-dimensional Gaussian function is:

$$\mathrm{g}(\mathrm{x},\mathrm{y};\mathrm{t}) = \frac{1}{2\pi t} e^{-\frac{(x^2+y^2)}{2t}} \quad (7)$$

As the variance t becomes larger, the smoothing effect of the image after filtering becomes more and more obvious, and the corresponding image also loses many details.

This problem can be solved by building an image Gaussian pyramid by down sampling. After obtaining the Gaussian pyramid, in order to find the stable and unchanging extreme points, use the Gaussian difference equation

The difference of Gaussian DOG (Difference of Gaussian) pyramid is established by subtracting two adjacent layers (as shown in Figure 2-3). The Gaussian difference equation $\mathrm{D}(\mathrm{x},\mathrm{y},\sigma)$ is the difference between two adjacent images of adjacent scales, as formula (8):

$$\mathrm{D}(\mathrm{x},\mathrm{y},\sigma) = \big(\mathrm{G}(\mathrm{x},\mathrm{y},\mathrm{k}\sigma) - \mathrm{G}(\mathrm{x},\mathrm{y},\sigma)\big) * \mathrm{I}(\mathrm{x},\mathrm{y})$$
$$\mathrm{D}(\mathrm{x},\mathrm{y},\sigma) = \mathrm{L}(\mathrm{x},\mathrm{y},\mathrm{k}\sigma) - \mathrm{L}(\mathrm{x},\mathrm{y},\sigma) \quad (8)$$

The reason for adopting the method of Gaussian difference is that the Gaussian difference algorithm approximates the Laplacian of Gaussian algorithm LOG (Laplacian of Gaussian). The Laplacian of Gaussian is a very stable feature extraction method. The so-called LOG is the image Second derivative, able to detect the fixed point of the image at different scales.

After obtaining the Gaussian difference pyramid, in order to find the point of interest in the image, we need to find the local extremum in the 3×3 neighborhood, and add the pixel value of the center point to 8 in the scale space plus two adjacent scales 18 adjacent pixels in the space. If the center point is greater than the surrounding 26 pixels, then the center point is the local extremum, this point is the extremum point, and so on to find all extremum points.

Number section and subsection headings consecutively in Arabic numbers and type them in bold. Use point size 10 for section headings and 10 for subsection headings. Avoid using too many capital letters. Keep section and subsection headings always flushed left. If any further subdivision of a subsection is needed the titles should be 10 point.

3.3. Specify direction for feature points

Analyze the gradient direction distribution characteristics of the pixels near the key points, and specify the direction parameters for the key points, so that the operator has rotation invariance.

$$\theta(x,y) = \arctan\{[\tfrac{(L(x,y+1)-L(x,y-1)]}{[L(x+1,y)-L(x-1,y)]}\} \quad (9)$$

3.4. Generate SIFT feature vector and feature point matching

Each seed point is composed of an 8-dimensional vector, so a feature point is represented by a 16×8=128-dimensional vector. The final 128-dimensional vector is the descriptor of the SIFT feature. The SIFT feature points at this time have removed geometric factors such as translation, scale transformation, and rotation.

In the SITF algorithm, a search algorithm based on the nearest neighbor method of feature points is adopted. The nearest neighbor method is an effective method to find matching points for feature points. The nearest neighbor point is the point with the shortest Euclidean distance from the invariant descriptor vector of the feature point. Figure .3 shows all the matching points obtained by the SITF algorithm.

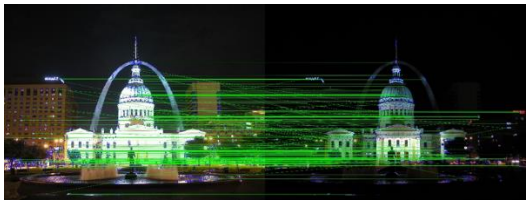


Fig.2 SIFT feature point matching point found by nearest neighbor method

4. Conclusions

In this paper, we have used two different methods to try to register the image, and both have good results. Each method has its own advantages and disadvantages. We should judge which algorithm to use according to the actual application scenario.

MTB is simpler and less costly, while SIFT algorithm is more complex, but the effect is higher. There are other algorithms worthy of in-depth study like SURF [4] and Registration algorithm based on Fourier transform [5], which are my next research directions.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, the project of Science and Technology Department of Chongqing Municipality, Chengdu Chengdian Network Technology Co., Ltd., Chengdu Civil-military Integration Project Management Co., Ltd., and Sichuan Yin Ten Gu Technology Co., Ltd.

References

[1] Greg Ward. Fast, Robust Image Registration for Composition High Dynamic Range Photographs from Handheld Exposure[J]. Journal of Graphics Tools, 2003, 8(2):17-30

[2] DAVID G. Lowe. Distinctive Image Feature from Scale-Invariant Key points[J]. International Journal of Computer Vision 60(2),91-110,2004

[3] A. Tomaszewska. Image Registration for Multi-exposure High Dynamic Range Image Acquisition[C]. WSCG2007

[4] Herbert Bay. Speed-Up Robust Feature (SURF)[J]. Computer Vision and Image Understanding 110 (2008) 346-359

[5] 强赞霞，彭嘉熊，王洪群.基于傅里叶变换的遥感图像配准算法[J].红外与激光工程.2004 vol.33No.4

A SIMPLE TERAHERTZ POLARIZATION-EXCITATION-BASED METHOD FOR MEASURING REFRACTIVE INDEX OF PLANAR MEDIUM

ZHU WENQUAN[1], LI PING[1,2], DING LI[1,2]

[1]University of Shanghai for Science and Technology, No. 516 JunGong Road, Shanghai 200093, China
[2]Terahertz Technology Innovation Research Institute, Shanghai, 200093, People's Republic of China
E-MAIL: zhuwenquan2009@126.com, sunnylding@163.com

Abstract:

In the present study, a simple Terahertz(THz) polarization-excitation-based method is proposed to examine the refractive index of planar medium. This method is devised for low THz band (i.e., 0.2 THz). Inspired by classical Fresnel formula, the method utilizes circularly polarized antenna to excite circularly polarized wave. Then, the reflected s-polarized wave and p-polarized wave are directly received through respective linearly polarized antenna. The refractive index thus can be easily obtained from the Brewster's angle of the object, which is the incident angle yielding the maximal s-component to p-component ratio. The overall measurement reliability is guaranteed from both the transmitting end and the receiving end. The transmitted THz wave is collimated and focused through the properly optical path for anti-interference, while the s-component and the p-component are received based on two balanced paths against the stimulation and disturbance. A high-resistance silicon is taken as a specimen, whose refractive index is estimated as 3.37 on average in 75 GHz-110 GHz band. This high agreement with the result measured by THz time domain spectroscopy verifies the effectiveness of the proposed method.

Keywords:

Polarized THz wave; Refractive index;Fresnel formula; Brewster's angle

1. Introduction

Terahertz (THz) is the electromagnetic wave region between microwave and the infrared, generally considered as the frequency going from 0.1 to 10 THz [1-6]. Recently a booming development in various THz applications, e.g., security imaging [3], nondestructive testing [4], THz spectroscopy [5], biomedical imaging/detection [6], etc., requires an urgent demand for electromagnetic parameters measurement of dielectric materials over THz band [7-8].

THz time domain spectroscopy (THz- TDS) has been widely used for decades to test planar materials through transmission and reflection techniques [5-8]. Among those work, it is obvious to observe that the starting frequency of the reliable spectrum of THz-TDS usually begins with 0.2 THz, even much higher. The limited band-width of the photoconductive antenna which is popularly used in THz-TDS may account for it [9-10]. Therefore, in low THz band, especially referring to the frequency between 0.1 THz-0.2 THz, the planar material measurements can be developed from the electronics sides. The classically well-known methods of electromagnetic parameters measurement in the microwave band include transmission line method, resonant cavity method, single probe method and the free space method [11-13]. However, the former three methods are hard to implement in low THz band due to the lack of suitable fixture/holder and the difficulty in sample fabrication. The fourth one, the free space method who sets least amount of constraints on sample size and environments, can potentially evaluate a sample in a non-contact fashion in THz band [14-16]. The authors in [14] utilized the metal MUT (material under test) holder with a circular hole on each side to reduce edge diffraction effect of MUT holder in the W-band free-space system for measuring the transmission coefficients. The authors in [15] proposed a scanning free-space measurement setup for the evaluation of microwave absorption properties of microwave absorbing materials. However, those free-space methods in a transmission-fashion way would suffer from the multi-value problem due to the thickness-resonance problem [16]. Therefore, we can have that the above mentioned methods cannot work straightforwardly in the low THz band (60.2THz) due to the bandwidth limitations of photoconductive antenna in THz-TDS, the lack of fixtures/holder, the difficulties in making samples or the multi-value problem in conventional microwave solutions.

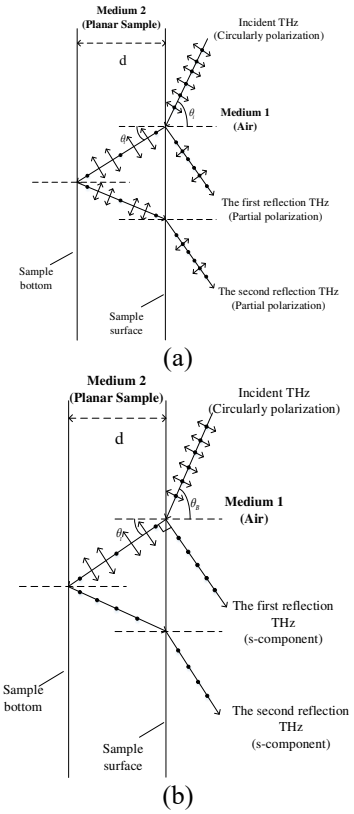


Fig. 1 Reflection and refraction between medium 1 and medium 2. (a) incidence with any angle θ_i , (b) incidence with Brewster angle θ_B

Motivated by the above considerations, this paper aims to propose a simple measurement method in lower THz band, called as THz polarization-excitation-based method, which can be easily implemented in laboratory. This method works in a reflection fashion to avoid the multi-value problem and is devised based on polarization measurement for breaking the rigid constraints on sample, fixture and environment by conventional methods. It is a kind of free space method and provides an easy way to implement the refractive-index measurement. Inspired by Fresnel formula in classical optics, this method achieves to measure refractive index of planar medium by finding its Brewster's angle. Specifically, it utilizes one circularly polarized transmitter to simulate the unpolarized incident wave and two orthogonal linearly polarized receivers to separately receive the s-polarized component and the p-polarized component of the echo reflected on the sample surface. A rotating mechanism consisting of two rotary platforms makes the movement of the sample and the receiver synchronously, to equivalently achieve the incident angle variation. The Brewster's angle of the sample then can be derived from the incident angle which corresponds to the maximum of the received s-component to the received p-component ratio. The refractive index therefore can be estimated by Fresnel formula when the first medium is air in free space. Moreover, this reflection-fashion measurement makes it perform anti-interference because of the balanced paths between the s-polarized component and the p-polarized component. Due to the geometry of the whole experiment, this proposed method can have the effective range of incident angle as [45°,90°], so does the Brewster's angle. This gives the ability to measure the refractive index over [1.2,5.5] by our proposed method. Experiments are implemented to achieve the THz wave transmitting and receiving by a Keysight Technolgies performance network analyzer (PNA) and two Virginia Diodes (VDi) THz extension modules. Two specimens are high-resistance silicon slice and a metal plate, while the metal plate is taken as a reference. The average estimated refractive index of silicon sample as 3.37 in 75 GHz-110 GHz band has shown the effectiveness of the proposed method.

2. Measurement Principles

Refractive-index measurement is one of the most basic physical quantities of electromagnetic characteristics of materials. As Fig. 1 shows, when electromagnetic waves are incident on one medium from another medium, reflection and refraction would occur at the interface according to the law of reflection and refraction. The incident wave consists of a pair of orthogonal electric-field components, where one vibration direction perpendicular to the incident surface is called the s-component, and the other vibration direction parallel to the incident surface is called p-component. The Fresnel formula [17] gives the expressions of the reflection and transmission coefficients of the s- and p-components when the wave is incident from medium1 to medium2, i.e.,

$$\mathrm{r}_{12}^{s}(\theta_i)=\frac{n_1\cos\theta_i-n_2\cos\theta_t}{n_1\cos\theta_i+n_2\cos\theta_t},\mathrm{r}_{12}^{p}(\theta_i)=\frac{n_2\cos\theta_i-n_1\cos\theta_t}{n_2\cos\theta_i+n_1\cos\theta_t}$$
$$\mathrm{t}_{12}^{s}(\theta_i)=\frac{2n_1\cos\theta_i}{n_1\cos\theta_i+n_2\cos\theta_t},\mathrm{t}_{12}^{p}(\theta_i)=\frac{2n_1\cos\theta_t}{n_2\cos\theta_i+n_1\cos\theta_t} \quad (1)$$

Where n_1 and n_2 is the refractive index of medium 1 and medium 2, respectively; θ_i and θ_t is the incident angle and the refraction angle, respectively; r_{12}^{s}, r_{12}^{p}, t_{12}^{s} and t_{12}^{p} denote the reflection coefficient of s-component, the reflection coefficient of p-component, the transmission coefficient of s-component and the transmission coefficient of p-component when the electromagnetic wave is incident from medium 1 to medium 2, respectively.

Similarly, when the electromagnetic wave is incident from medium 2 to medium 1, we can have

$$\mathrm{r}_{21}^{s}(\theta_i)=\frac{-n_1\cos\theta_i+n_2\cos\theta_t}{n_1\cos\theta_i+n_2\cos\theta_t},\mathrm{r}_{21}^{p}(\theta_i)=\frac{-n_2\cos\theta_i+n_1\cos\theta_t}{n_2\cos\theta_i+n_1\cos\theta_t} \quad (2)$$
$$\mathrm{t}_{21}^{s}(\theta_i)=\frac{2n_2\cos\theta_i}{n_1\cos\theta_i+n_2\cos\theta_t},\mathrm{t}_{21}^{p}(\theta_i)=\frac{2n_2\cos\theta_t}{n_2\cos\theta_i+n_1\cos\theta_t}$$

Where r_{21}^{s} , r_{21}^{p} , t_{21}^{s} and t_{21}^{p} denotes the reflection coefficient of s-component, the reflection coefficient of p-component, the transmission coefficient of s-component and the transmission coefficient of p-component when the electromagnetic wave is incident from medium 2 to medium 1, respectively.

Assuming the incident signal intensity is 1, the intensity of s- and p-compo nents finally received by the receiver at the side of medium 1 are

$$\begin{aligned} R^{s}(\theta_i)&=r_{12}^{s}(\theta_i)+t_{12}^{s}(\theta_i)\cdot r_{21}^{s}(\theta_i)\cdot t_{21}^{s}(\theta_i)\\ R^{p}(\theta_i)&=r_{12}^{p}(\theta_i)+t_{12}^{p}(\theta_i)\cdot r_{21}^{s}(\theta_i)\cdot t_{21}^{p}(\theta_i)\end{aligned} \quad (3)$$

Where R^{s} and R^{p} are the amplitude of reflected s-component and reflected p-component, respectively.

3. Measuring Method

According to Fresnel formula, there is a Brewster's angle, denoted as θ_B . When the electromagnetic wave enters the dielectric surface with the incident angle as θ_B , it can give a zero reflected p-component, i.e., $r_{12}^{p}(\theta_B)=r_{21}^{p}(\theta_B)=0$, shown as dotted line in Fig. 1 (b).

Therefore, according to (1) or (2) and the refraction law, the refractive index of medium 2 can be obtained as follows

$$n_2=n_1\tan\theta_B \quad (4)$$

Thus, the refraction index of medium 2 can be directly derived from the Brewster's angle and the known refraction index of medium 1. Thus we would have (3) as

$$\begin{aligned} R^{s}(\theta_B)&=r_{12}^{s}(\theta_B)+t_{12}^{s}(\theta_B)\cdot r_{21}^{s}(\theta_B)\cdot t_{21}^{s}(\theta_B)\\ R^{p}(\theta_B)&=0\end{aligned} \quad (5)$$

Inspired by (4) and (5), the schematic of the THz polarization-excitation-based free space method for refractive-index measurement of planar medium is shown in Fig. 2. The experiment adopts the reflective measurement method. Medium 1 is air, i.e., $n_1=1$, and medium 2 is the planar sample under the test. In transmitting, THz waves is generated by the combination of the radio frequency generator, i.e., PNA (**A**) and the multiplier, i.e., VDi extender (**B**), and is transmitted by a circularly polarized antenna (**C**). The transmitted THz wave will be collimated and focused on sample surface(**G**) through the optical path who consists of the parabolic mirror 1 (**D**), 2 (**E**) and 3 (**F**). The reflected signal is then received by the receiver (**J**), who is achieved by another VDi extender. It is equipped with the linearly polarized antenna (**K**) to make a time-sharing measurement

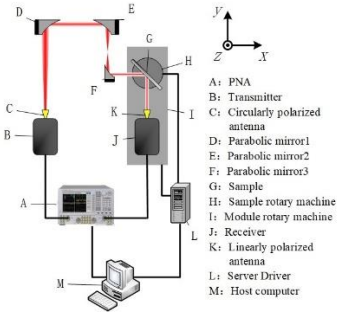


Fig.2 Schematic of the measurement.

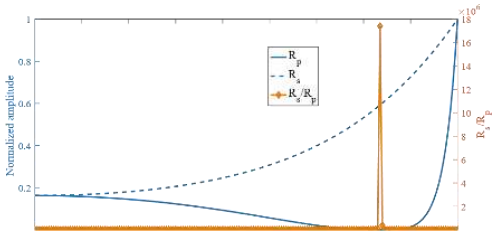


Fig.3 Simulation of an example with refractive index $n_2=3.4$ and Brewster's angle $\theta_B=73.6^{\circ}$

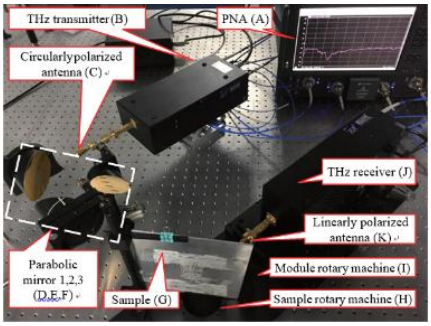


Fig.4 Photography of the experimental setup.

of the reflected s-component by horizontally linear-polarization antenna and the reflected p-component by virtually linear-polarization antenna, respectively. A sample-rotary platform (**H**), on which the sample is fastened, together with the receiver (**J**) is positioned on another module-rotary platform (**I**). The synchronous movement of the sample rotary platform (**H**) and the module rotary platform (**I**) is controlled by the host computer (**M**) through their respective server driver (L). Both the movements of the platforms equivalently achieve the change of incident angle.

After collecting the reflected signals over a range of incident angles, examining the maximal ratio of the reflected s-component over the p-component can locate the Brewster's angle θ_B , i.e.,

$$\theta_B = \max_{\theta_i} \left\{ \frac{R_s(\theta_i)}{R_p(\theta_i)} \right\} \tag{6}$$

Therefore, the medium 2 can be estimated by (4) if the refractive index of medium 1 is give, e.g., $n_1 = 1$ for air.

For example, when there is a material with refractive index of 3.4, its Brewster's angle can be computed as $\theta_B = 73.6^\circ$. We simulate its s-component and p-component

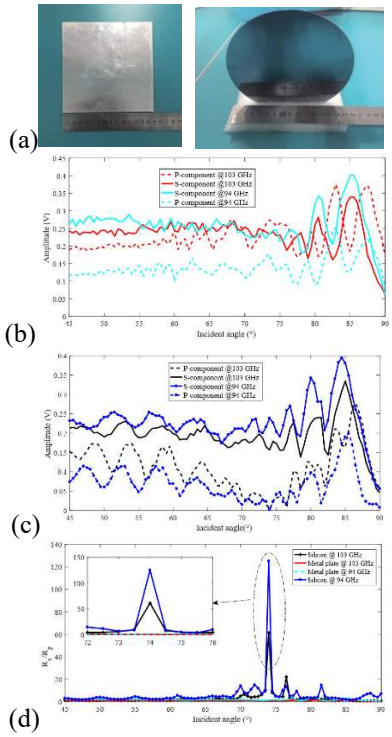


Fig.5 Experiment Results at frequency of 88 GHz and 94 GHz. (a)The photograph of sample, left-metal plate, right-silicon slice, (b)The reflected amplitude of silicon slice, (c) the reflected amplitude of metal plate, (d) the computed ratio.

based on (3) when θ_i varies from 0° to 90° with the step of 1°, shown in Fig. 3 the with left coordinate system. Then the Brewster's angle can be estimated based on (5) as $\theta_B = 74^\circ$, as Fig. 3 shows with the right coordinate system. The accuracy is affected by the gridding of angle dimension. Therefore, decreasing the step angle can increase the estimation accuracy of Brewster's angle.

4. Experiments

The experiment is shown in Fig. 4 with low constraints on the environment. The PNA is Keysight Tech. N5222B, and VDi extender is chosen for 75 GHz-110 GHz band. Both the rotary motors are OSM-160 YAW by Optosigma. The parabolic mirror 1 (**D**) and the parabolic mirror 2 (**E**) are with the diameter of 3 inches and the reflected effective focal length (EFL) of 3 inches, while the parabolic mirror 3 (**F**) is with the diameter of 2 inches and the reflected EFL of 2 inches. Considering the physical limitation of the receiving movement, the rotating mechanism consisting of the sample rotary platform (**H**) and the module rotary platform (**I**) can efficiently test the range of incident angle over [45° ,90°]. This implies $\theta_B \in [45^\circ, 90^\circ]$.Therefore, according to (4), we can use this method in free space (i.e., medium 1 is air and $n_1 = 1$) to quickly measure the sample whose refractive index is in [1.2,5.5].

The room temperature is 25°C and humidity is 30%. The system works in frequency sweep mode, and the step of incident angle is set as 0.5°. As Fig. 5 (a) shows, the first specimen is a metal plate, taken as a reference with no Brewster's angle, and the second specimen is a high-resistivity silicon slice, whose refractive index is already known as 3.4 by THz-TDS in 0.2 THz-3 THz in [5]. Based on (4), the measured s-component, p-component and the computed ratio versus incident angle are shown in Fig. 5 (b), (c) and (d). (b) and (c) show the recorded amplitude of s-component and p-component at frequency of 88 GHz and 94 GHz for metal plate and silicon slice, respectively. By computing the ratio shown in Fig. 5 (d), we can see that there is no Brewster's angle of the metal plate and its ratio in (4) is almost a constant. This is because metal plate has a well-known ideal mirror reflection, both the reflected s-component and p-component keeps the similar activity of change. As to the silicon slice, Fig. 5 (c) shows that its maximal ratio happens at the incident angle of 74°, i.e., $\theta_B = 74^\circ$. Bringing $\theta_B = 74^\circ$ and $n_1 = 1$ into (4), the refractive index of this silicon slice is estimated as 3.48 at both the frequency of 88 GHz and 94 GHz.

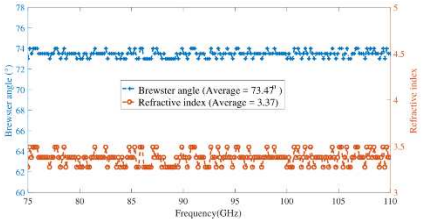


Fig. 6 The estimated Brewster angle and refractive index with varying frequency for silicon slice.

Furthermore, the relationship of Brewster's angle of silicon slice by (5) and that of the estimated refractive index by (4) versus frequency is examined in Fig. 6. We can have that over 75 GHz -110 GHz band, the variation of Brewster's

angle versus frequency is in [73.5°, 74.5°] and its average is 73.47°. Then, the corresponding refractive index with varying frequency is in [3.28,3.49] and its average is 3.37. The agreement with the measured refractive index of silicon as 3.4 by THz-TDS in [5] and [17] really verifies the effectiveness of our proposed method.

5. Conclusion

In this paper, a simple THz polarization-excitation-based method has been proposed. This method is devised to fill the gap of measurement difficulty in low THz band (i.e., 6 0.2THz), no matter by the conventional microwave methods or by THz-TDS. Based on well-known Fresnel formula, the method is simple to build up experiment platform by utilizing the polarization measurement technique and obviously puts less constraints on the experiment setting. Both the simple optical paths for transmitting and two balanced paths for receiving make the proposed method have anti-interference performance. They guarantee the reliability of the measurement. The results in experiment section are obtained in a single experiment. This verifies the effectiveness of the proposed method to easily implement the refractive-index measurement of planar medium in low THz band. Although the experiment is conducted on 75 GHz-110 GHz band, the proposed method in principle can work well on other THz band.

Acknowledgements

This work was supported in part by the National key R&D Program of China (2018YFF01013003), in part by the National Natural Science Foundation of China (61731020, 61605113, 61601291), in part by the 111 Project (D18014)

References

[1] B. Ferguson and ZHANG, 'Materials for terahertz science and technology', Physics, 2003, 1, pp. 26–33

[2] N. Ghalichechian and K. Sertel, 'Permittivity and loss characterization of su-8 films for MMW and terahertz applications', IEEE Antennas & Wireless Propagation Letters, 2015, 14, pp. 723–726

[3] J. F. Federici, B. Schulkin, F. Huang, D. Gary, R. Barat, F. Oliveira, and D. Zimdars, THz imaging and sensing for security applications ÅĆ explosives, weapons and drugs', Semiconductor Science Technology, 2005, 20, pp. 0–0

[4] J. Christian, W. Steffen, P. Ole, S. Maik, V. Nico, S. Mohammed, K. Norman, J. Christian, H. Thomas, and K. Martin, 'Terahertz imaging: applications and perspectives', Applied Optics, 2010, 49, pp. 48–57

[5] P. Ioachim, W. Rafal, and K. Martin, 'Highly accurate optical material parameter determination with THz time-domain spectroscopy', Optics Express, 2007, 15, pp. 4335

[6] G. P. Gallerano, G. S. Park, A. Ramundo-Orlando, and O. Zeni, 'Guest editorial: Special issue on thz radiation applied to biophysical, biological, and biomedical sciences', Journal of Infrared Millimeter & Terahertz Waves, 2018, 39, pp. 1–2

[7] J. M. Seligman, 'Spectral characterization of dielectric materials using terahertz measurement systems', Dissertations & Theses-Gradworks, 2015

[8] A. Buzdy, M. Unferdorben, G. Tth, J. Hebling, I. Hajdara, L. Kovcs, and L. Plfalvi,' Refractive index and absorption coefficient of undoped and mg-doped lithium tantalate in the terahertz range', Journal of Infrared Millimeter & Terahertz Waves,2017,18, pp. 1–9

[9] R. Mendis, C. Sydlo, J. Sigmund, M. Feiginov, P. Meissner, and H. L. Hartnagel,' Spectral characterizeation of broadband THz antennas by photoconductive mixing: toward optimal antenna design', IEEE Antennas & Wireless Propagation Letters, 2005, 4, pp. 85–88

[10] Y. Zhang, X. Zhang, S. Li, J. Gu, Y. Li, Z. Tian, C. Ouyang, M. He, J. Han, and W. Zhang, 'A broadband THz-TDS system based on DSTMS emitter and LTG InGaAs/InAlAs photoconductive antenna detector', Scientific Reports, 2016, 6, pp. 26949

[11] Y. B. Feng, Measurement of electromagnetic parameters for microwave absorbing materials using transmission/reflection method', Chinese Journal of Radio Science, 2006, 21, pp. 293–297

[12] A. Elhawil, G. Koers, L. Zhang, et al., 'Reliable method for material characterisation using quasi-optical free-space measurement', Iet Science Measurement & Technology, 2009, 3(1), pp. 39–0.

[13] P. Lederer, S. Szwarnowski, T. Hodgetts,' Measurement of cross-polar transmission in free space', IET Science, Measurement & Technology, 2006, 153(6), pp. 216–0.

[14] J. S. Kang, J. H. Kim, and J. I. Park, 'Reduction of edge diffraction effects of MUT holder using em absorber in W-band free-space material measurements', in International Symposium on Antennas and Propagation, 2007

[15] H. Ahmed, J. Hyun, and J. R. Lee, 'Development of scanning single port free space measurement setup for imaging reflection loss of microwave absorbing materials', Measurement, 2018, 125

[16] H. U. Da-Hai, R. Zhao, D. U. Liu-Ge, and Y. H. Wang, 'The permeability and permittivity measure-

ment technique of flat substrate materials at terahertz', Journal of Microwaves, 2016
[17] M. Born, E. Wolf and E. Hecht, 'Principles of Optics: Electromagnetic Theory of Propagation, Interference and Diffraction of Light', Physics Today, 2000, 53(10), pp. 77–78.

INDEPENDENTLY TUNABLE DUAL-BAND BANDPASS FILTER

AIDOO MICHAEL WILSON[1], AYIVI WILLIAM[2], WIREKOH-TAWIAH ALBERT[2]

[1]Electronic Science and Engineering, University of Electronic Science and Technology of China, Sichuan, Chengdu
[2]School of Electronic Science and Engineering, University of Electronic Science and Technology of China.
E-MAIL: mwilsonaidoo@outlook.com, williamsayivi@gmail.com, krowtail@outlook.com

Abstract:

A reconfigurable multiband band-pass filter is proposed in this paper, using the structures and techniques of the Stub-loaded Stepped-Impedance Resonators dual-mode configuration. This design uses the source-load link and the shorted T-shaped stub lines. The proposed structure has the advantages of compact size, high selectivity, and a single control bias voltage applied. Four adjustable transmission zeroes were attained by the suggested filter, with more than 40 dB rejection between the two passbands. Employing the coupling paths effectively yielded the independent control of the two passbands. For the purpose of tuning, two identical varactor diodes were loaded onto the open ends of the resonators. A frequency tuning range of 1.08 GHz to 1.5 GHz and 1.99 GHz to 2.7 GHz is achieved in the two passbands respectively. The designed filter realized an insertion of 1.2 dB to 1.32 and 0.86 dB to 1.11 dB respectively in the tuning process. The overall filter size of $0.13\lambda_0 \times 0.03\lambda_0$ is achieved.

Keywords:

Stub-loaded stepped-impedance resonator (SLSIR); Reconfigurable filter; Bandpass filter (BPF); Microstrip; High selectivity; Transmission zeroes (TZ)

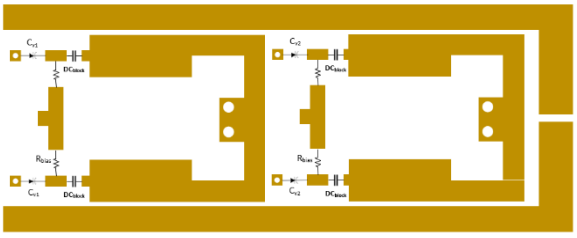
1. Introduction

The increase in the number of applications in the wireless communication system has made it necessary, the design of filters with multi-band functions. Currently, the drawbacks in some aspects namely, poor insertion and return losses, interference of the spurious frequency during the tuning of the center frequency, poor frequency selectivity, and low-frequency tuning range have been counted in several reports, which needs more inputs of work in the research work. For this, several reports have been studied on BPFs [1-8].

Reconfigurable bandpass filters have in recent times become the talk of the moments, attracting several investigations and reports. In a quest to realize a BPF with tunable functionality, a two-way independently designed and cascaded approach was employed in [1], for the achievement of the lower and higher frequency cut-off efficiency. Meanwhile, the techniques of stepped-impedance resonators (SIR) and SLSIR have also been adopted in designing a dual-band BPF in [3][5], both with the tri-mode structure, and exploiting the advantages that come with the dual coupling paths. A report has been uncovered in [8] where short parallel-coupled lines are used to design a BPF with tuned frequencies and bandwidths. The stub-loaded theory and application were investigated in [7], designing a dual-band BPF with independent control of the bandwidths and frequencies.

The study of these earlier reported papers leaves adequate information on the fact that though the trends have designs with good filter characteristics, there is still the need for improvement with the current dynamism of trends and technical demands. This paper reports on a reconfigurable dual-band BPF function, through the use of SLSIR and a single bias voltage supply at each filter side for effective tuning.

Fig.1 The layout of the proposed dual-band bandpass filter



with SLSIR configurations and the varactor circuits.

The proposed filter is symmetrically structured and has similar parameters at both resonators. Carefully and technically studying this configuration it was prudent to vary the varactors installed at the openings of the resonators as illustrated in Figure 1. Hence the passbands' frequency of the filter can be widely changed. To demonstrate, the proposed dual-band tunable bandpass filter is designed and executed in order to verify the proposed idea.

2. Circuit design

The model circuit for the microstrip transmission line has been illustrated in Fig 2, together with its design specifications and optimized physical and electrical parameters for the study and analysis. Following its symmetrical nature, the even-and odd-mode analysis is used to establish the resonant frequencies.

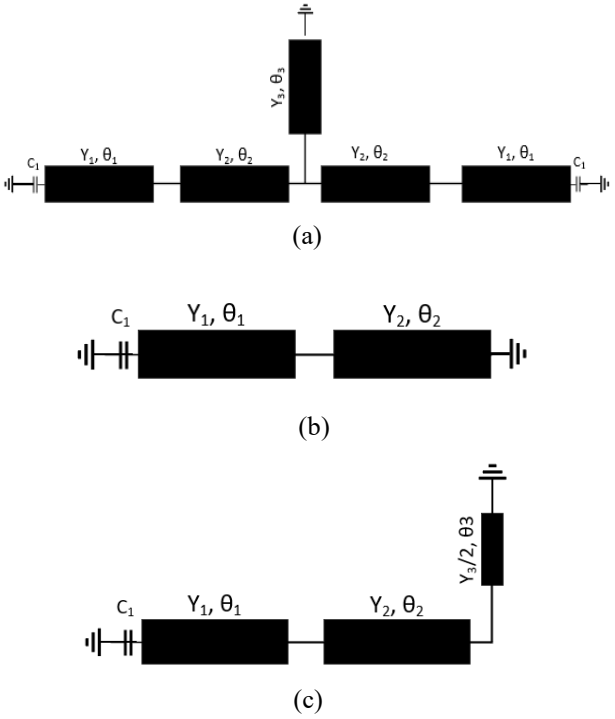


Fig. 2 (a) Circuit of the SLSIR structure. (b) Odd-mode equivalent circuit. (c) Even-mode equivalent circuit.

The model consists of a pair of a quasi T-shaped stub-loaded SIR dual-mode resonator with each loaded with two variable capacitances (varactors) and a shorted stub. The varactors are loaded at the open ends of each resonator. These two sections of the SLSIR are evenly coupled with the I/O lines. Also, the source to load (of the I/O lines) coupling is employed in this design to enhance the realization of the required coupling effects in order to achieve the desired bandwidth. Inherently, in the top stopband, the SLSIR dual-mode structure has a transmission (TZ). These TZs are toppled by the source-load coupling, which also adds more TZs in the lower stopband, which increases the number of TZs to four (4), indicating a high selectivity at each passband. Each passband has two TZs located at each end. The T-shaped stub technique, as a strategy, was employed to limit the complexity and the number of control voltages when installing the tuning devices.

A thorough study of the structure indicates that each resonator could generate two resonant modes. Thus, for each resonator, the even-and odd-modes are obtained in a similar way as reported in [9-11] as

$$Y_{in\_e} = j2\pi fC_{V1} + Y_2\left(\frac{Y_{load} + j\left(Y_2\tan\theta_2 + Y_1\tan\theta_1\right)}{Y_2 + jY_{load}\tan\theta_1\tan\theta_2}\right) \quad (1)$$

$$Y_{in\_o} = j2\pi fC_{V1} - jY_{load}\cot\left(\theta_t\right) \quad (2)$$

$$Y_{load} = \frac{Y_3}{2}.\frac{j\left(Y_3\tan\theta_3 + 2\pi fC_v\right)}{Y_1 - j\frac{Y_3}{2}\tan\theta_3 - j2\pi fC_v} \quad (3)$$

For the tunability effect in this filter design, a total of four identical varactors are loaded onto the open ends of the resonators, as depicted in Figure 1. The entire tuning circuit is designed such that it is controlled by only one type of control voltage for each passband, unlike the usual stub-loaded tunable filters that demand two types of control voltages

3. Results and analysis

Fig 3 illustrates the results simulated on HFSS, on Taconic RF35 substrate with a relative dielectric constant of 3.5, the thickness of 0.508mm, and a conductor thickness of 0.018mm. After optimization, the various dimensions with which the result was realized are as given below (unit: mm).

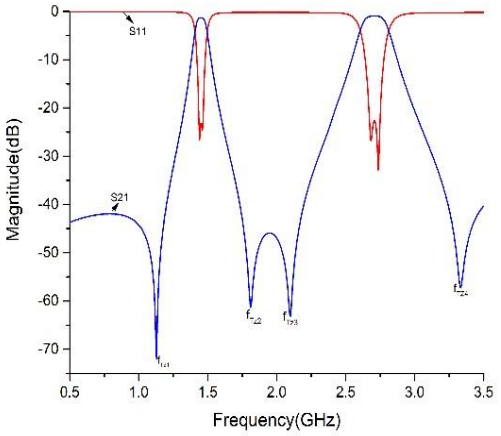
The design achieved an absolute bandwidth of 110MHz (±5MHz) and 220MHz (±5MHz), in the lower and higher frequency passbands respectively, as well as insertion loss varying from 1.2dB to 1.32dB and 0.86dB to 1.11dB in the lower and higher frequency passbands respectively, with the return loss more than 20dB in each passband. A frequency tuning range of 1.08GHz to 1.5GHz and 1.99GHz to 2.7GHz is achieved in the two passbands respectively.

Table1 Dimensions of the proposed filter

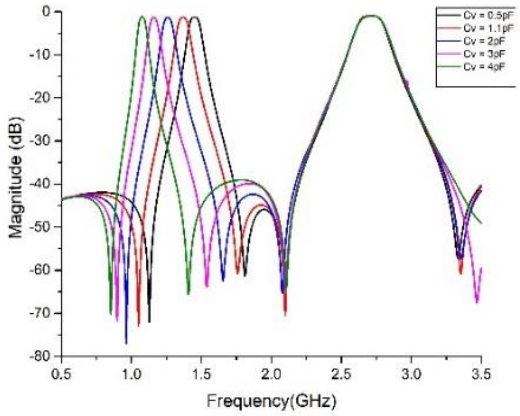
Filter	w_0	w_1	w_2	w_3	l_0	l_1
A	1.11	0.90	2.35	2.25	5.22	8.4
B	1.11	1.08	2.30	2.13	5.22	5.15
Filter	l_2	l_3	l_4	s_1	s_2	
A	13.0	8.05	1.4	0.16	0.2	
B	5.00	8.05	0.7	0.16	0.2	

After the design and optimization of the proposed filter, the results are as observed in the figure below with all the transmission zeroes shown. The various plots of the S11 and S21 are also displayed, showing the evidence of the practicality of the work. The two passbands were separately tunned to demonstrate the concept discussed and the

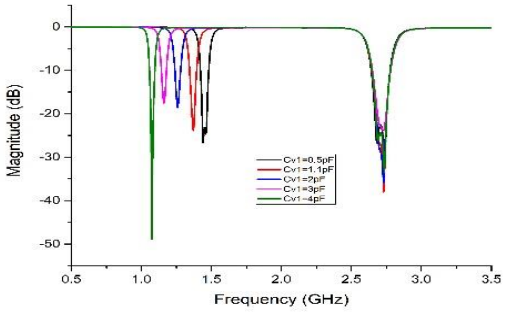
functions of the reconfigurability of our proposed multi-band bandpass filter.



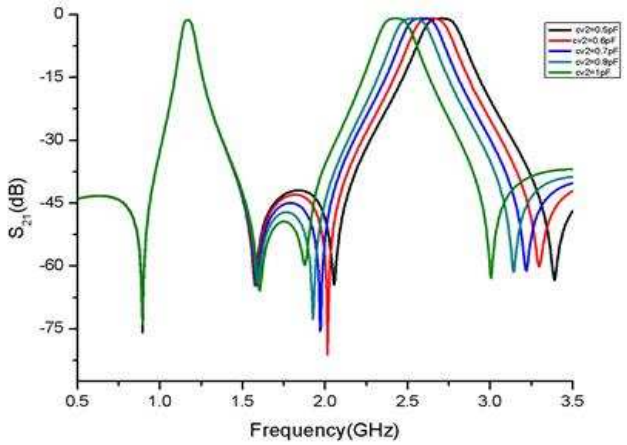
(a)



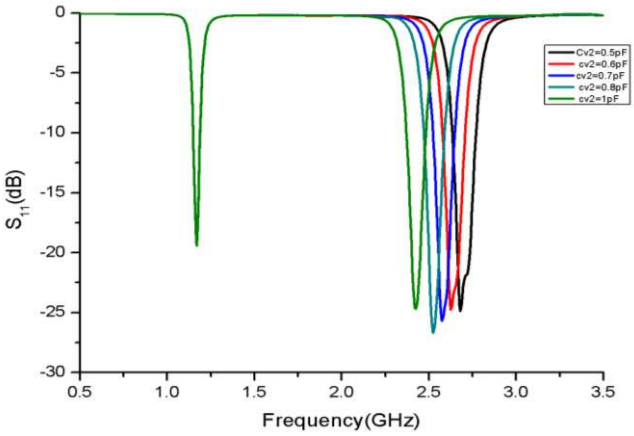
(b)



(c)



(d)



(e)

Fig.3 Plots of S-parameter results. (a) S-parameter results without tuning. (b) S_{21} plot of lower frequency passband tuning. (c) S11 plot of lower frequency passband tuning. (d) S21 plot of the higher frequency passband tuning. (e) S11 plot of the higher frequency passband tuning (in all tuning cases, the other passband remained fixed).

4. Conclusions

The results and other necessary features of the multi-transmission pole dual-band bandpass filter designed based on the theoretical framework of stub-loaded stepped-impedance resonators have been discussed in this paper. This study reported on a reconfigurable multi-band bandpass filter. This proposal has to an extent suggested a solution to the problems of the filter size, return loss, insertion loss, and independent tunability. It mainly reported on a design structure with two identical varactors in each filter. emp

References

[1] K. Song, M. Fan, and Y. Fan, "Novel Reconfigurable Bandpass Filter With Wide Tunable Bandwidth," *2019 IEEE MTT-S Int. Wirel. Symp. IWS 2019 - Proc.*, pp. 1–3, 2019, doi: 10.1109/IEEE-IWS.2019.8803933.

[2] G. Zhang, Y. Xu, and X. Wang, "Compact tunable bandpass filter with wide tuning range of centre frequency and bandwidth using short coupled lines," *IEEE Access*, vol. 6, pp. 2962–2969, 2017, doi: 10.1109/ACCESS.2017.2786296.

[3] C. Chen, "A Compact Reconfigurable Microstrip Dual-Band Filter Using Varactor-Tuned Stub-Loaded Stepped-Impedance Resonators," *IEEE Microw. Wirel. Components Lett.*, vol. 23, no. 1, pp. 16–18, 2013, doi: 10.1109/LMWC.2012.2235061.

[4] C. Ge and X. W. Zhu, "Highly-selective tunable bandpass filter with two-path mixed coupling," *IEEE Microw. Wirel. Components Lett.*, vol. 24, no. 7, pp. 451–453, 2014, doi: 10.1109/LMWC.2014.2316218.

[5] B. You, L. Chen, Y. Liang, and X. Wen, "A High-Selectivity Tunable Dual-Band Bandpass Filter Using Stub-Loaded Stepped-Impedance Resonators," pp. 1–3, 2014.

[6] R. Gómez-garcía, S. Member, and A. F. Section, "Dual-Behavior Resonator-Based Fully Reconfigurable Input Reflectionless Bandpass Filters," vol. 29, no. 1, pp. 2018–2020, 2019, doi: 10.1109/LMWC.2018.2884151.

[7] X. Wu, F. Wan, and J. Ge, "Stub-Loaded Theory and Its Application to Balanced Dual-Band Bandpass Filter Design," *IEEE Microw. Wirel. Components Lett.*, vol. 26, no. 4, pp. 231–233, 2016, doi: 10.1109/LMWC.2016.2537045.

[8] C. Zhu *et al.*, "Split-Type Dual-Band Bandpass Filters With Symmetric / Asymmetric Response," vol. 28, no. 1, pp. 2017–2019, 2018.

[9] J. Xu, "Compact Microstrip Tri-Band Bandpass Filter Using New Stubs Loaded Stepped-Impedance Resonator," *IEEE Microw. Wirel. Components Lett.*, vol. 26, no. 4, pp. 249–251, 2016, doi: 10.1109/LMWC.2016.2537740.

[10] Y. Xie, F. C. Chen, and Z. Li, "Design of dual-band bandpass filter with high isolation and wide stopband," *IEEE Access*, vol. 5, pp. 25602–25608, 2017, doi: 10.1109/ACCESS.2017.2773502.

[11] B. Pal and S. Dwari, "International Journal of Electronics and Communications (AEÜ) Microstrip dual-band bandpass filter with independently tunable passbands using varactor-tuned stub loaded resonators," vol. 73, pp. 105–109, 2017.

FINANCIAL TIME SERIES PREDICTION MODEL BASED RECURRENT NEURAL NETWORK

CHENG CHAOZHI[1], GAO YACHUN[1], NI JINGWEI[2]

[1]School of Physics, University of Electronic Science and Technology of China, 611731, China
[2]Department of Computer Science, The University of Hong Kong, Hong Kong
E-MAIL: chengchaozhi@std.uestc.edu.cn, gaoyachun@uestc.edu.cn, u3544680@hku.hk

Abstract:

Financial time series prediction is usually considered as one of the most difficult challenges because of huge external factors, which are usually stochastic and sensitive so that we can hardly recognize the patterns from historical information. Besides, traditional time series prediction models cannot adapt to the changes in financial circumstances. To overcome these problems, we design a prediction model based on recurrent neural network with gating units, which can learn historical information and adapt the market changes through a specific inner structure. Experiments carried on the Shanghai Securities Composite Index show that the prediction results of our model have more competitive performance compared to those of other traditional models. Our model has good interpretability, and the effects of model hyperparameters on prediction accuracy are also analyzed. On the basis, we proceed with the long-term trend analysis and estimate precisely the tipping points of the stock market. These results give application prospects in risk assessment and portfolio management for the finance industry.

Keywords:

Financial time series; Prediction model; Recurrent neural network

1. Introduction

Algorithms of time series prediction have been general studied in different fields, like economics, biology, meteorology, and specific applications including financial market prediction [1], weather prediction [2], complex dynamic system analysis [3], urban traffic flow prediction [4], and so on.

In the past decades, there are many mathematical models that aim to describe time series mechanisms like stochastic and volatility. The most representative works include the Autoregressive Model (AR), Move Average model (MA), and ARMA with the two models integrated [5]. After this, ARIMA has been proposed used to describe unstable time series [6]. However, to get better results, complex hypotheses are required, leading to poor universality of the models.

Recently, Machine Learning (ML) models, such as linear regression, support vector machine [7], random forest [8], have been paid much attention because of higher expressive ability and relatively better performances compared to the classical models. Within the ML field, Deep Learning (DL) is the most powerful predictor, which is a kind of artificial neural networks consisting of multiple processing layers.

On the basis, Recurrent Neural Network (RNN), a type of DL network, is designed for sequential data analysis like speech recognition [9]. RNN works through adjustment in internal parameters, which optimizes the loss function for date feature extraction and finally realizes the future prediction. Nowadays, RNN is widely applied for the prediction of various time series, such as traffic flow [4], exchange rate [12], chaos time series [3], etc. There are two weaknesses of RNN, i.e., the inability to learn long-term dependencies, and the exploding and vanishing gradients. To solve these problems, Gate Recurrent Unit (GRU) and Long-Short-Term Memory (LSTM) networks are designed.

Despite RNN performs well in most cases, the mechanism is hard to understand why it works well. As a result, it's difficult to build a simple and efficient network structure for specialized financial time series prediction. In this paper, we aim to address these problems by adding gating units in the cell of the RNN model, which is designed to adjust the influence weights of historical and current information at different time steps. We evaluate the prediction ability by testing the Shanghai Securities Composite Index (SSCI). The experimental results of both predicted financial prices and tipping points confirm the effectiveness and efficiency of our model. The performance of various hyperparameters in the model is tested as well. The main contributions of this paper are summarized as follows:

(1) We propose a RNN model based on specific gating unit

designed for financial time series prediction.
(2) A variety of hyperparameters setting of the model are tested to find influence factors.
(3) The prediction results are used to implement long-term trend analysis and tipping points searching.

2. Related Work

DL has successful applications in financial time series prediction [13-15]. For instance, spatial neural networks are designed to explore information from the Limit Order Book (LOB) for stock price prediction [16]. Convolution Neural Network (CNN) and RNN are both applied for analyzing large amounts of high-frequency financial trading orders and predicting the change of stock price [17-18]. Besides, LSTM is applied for predicting stock price trends, and before training LSTM mode, stock time series are processed by wavelet transform and stacking auto-encoder for feature extraction [19]. Furthermore, Temporal Attention-augmented Bilinear Network (TABL) adds attention mechanism in a condensed forward neural network for financial time series prediction [20].

Nevertheless, though the competitive performance of DL has been proved in these works, it can hardly obtain the mechanism of the training targets of each hidden layer, making it difficult to explain the features of each layer. Here, we build a specific RNN cell structure, which is used to train influence weights and can adjust the weights according to learning historical and current price information. Results shows the model has good interpretability and adaptability.

3. Model

Consider a financial time series of stock trading prices $\{p_t|t = 1,2, \dots T\}$, Our goal is to make a 1-step prediction on p_{t+k+1} based on the history prices from p_t to p_{t+k}. Formally, the 1-step prediction formula is below:

$$p_{t+k+1} = f(p_t, p_{t+1}, \dots, p_{t+k}) \quad (1)$$

In Eq. (1), function f denotes the model, which maps the history prices to future price. $[p_t, p_{t+1}, \dots, p_{t+k}]$ is a k-dimensional vector for function input, p_{t+k+1} is a scalar for function output.

First, we can build an explicable and traditional linear regression prediction model for function f, which can capture first-order linear correlation with historical data:

$$p_{t+k+1} = w_0 p_t + w_1 p_{t+1}, \dots, w_k p_{t+k} + b \quad (2)$$

Once the model has been trained, the parameters are determined and cannot be modified. As a result, when the financial market changes, the model will give bad prediction.

In order to fix this problem, we change the function f to the formula as below:

$$p_{t+k+1} = \sum_{i=1}^{k} w_i(p_t, p_{t+1}, \dots p_{t+i}) * p_{t+i} + b(p_t, \dots p_{t+k}) \quad (3)$$

We change the constant parameters w, b in Eq. (2) to functions w, b of history prices in Eq. (3). From the equation, when the market environment remains unchanged, the values of w and b remain the same, and in few time steps when the market environment changes, the values of w and b will change accordingly. Consequently, the new RNN model with

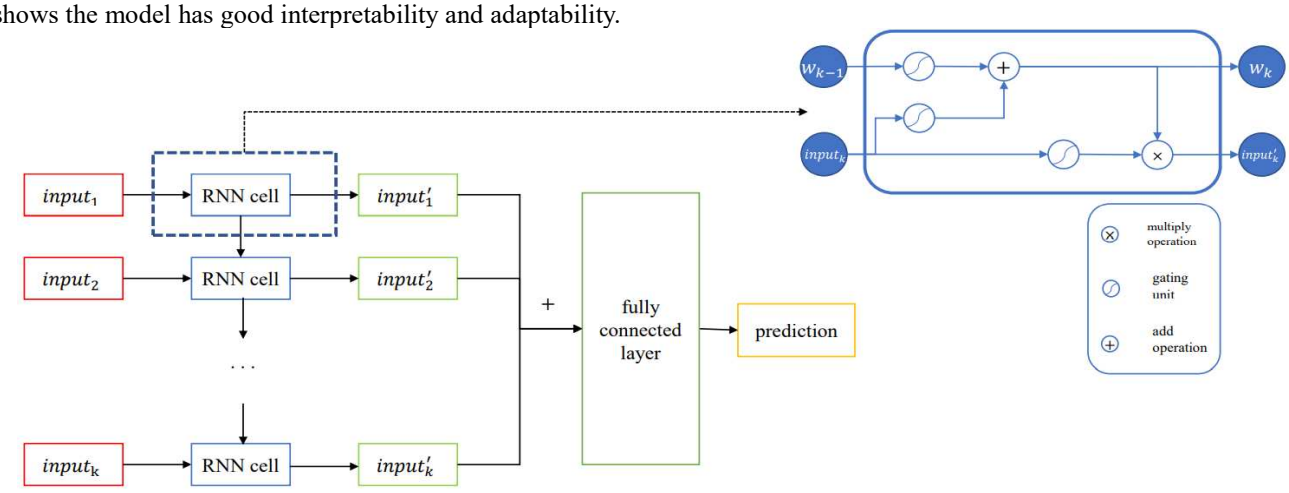


Fig.1 The schematic descrition of finnaical time series predction model

specialized RNN cell structure is designed for judging the variation of financial market environment from weight function w and bias function b.

In Figure 1, $input_k$ is the k-th input of RNN, corresponding to p_{t+k} in Eqs. (1-3). And $input'_k$ is the k-th output of RNN, which is $w_k(p_t, p_{t+1}, \dots p_{t+k}) * p_{t+k}$ in Eq. (3) above. After k times recurrence we can get totally k $input's$, and calculate $sum = \sum_{i=1}^{k} w_i(p_t, p_{t+1}, \dots p_{t+i}) * p_{t+i}$. Next, according to Eq. (3), the predicted result p_{t+k+1} is obtained by adding the result of function b through a

fully-connected layer to the value sum.

The vital component of our model is the RNN cell. RNN cell is designed specifically to learn complicated and nonlinear historical information and can adapt to the influence of financial market changes. The calculations in the RNN cell are as follows:

$$w_k = tanh(W_1 input_k + b_1) + tanh(W_2 w_{k-1} + b_2) \quad (4)$$

$$input'_k = tanh(W_3 input_k + b_3) * w_k \quad (5)$$

Here, $w_k = w_k(p_t, p_{t+1}, \dots p_{t+k})$, **W** is a matrix and **b** is a biased vector. And $\mathbf{tanh}()$ is gating unit function defined as:

$$\tanh x = \frac{\sinh x}{\cosh x} = \frac{e^x - e^{-x}}{e^x + e^{-x}} \quad (6)$$

Compare to traditional *sigmoid* gating unit function, the output of which is restricted to [0,1], *tanh* function can expand the range to [-1,1]. Because in financial market, w_k, the influence weight of historical prices, can be either positive or negative, *tanh* function is more proper here. Besides, the Taylor expansion of *tanh* function gives infinite high degree polynomials, which makes it possible to simulate arbitrary nonlinear function patterns.

In Eq. (4), the influence weight of current information w_k is affected by both current input $input_k$ (the first term in the equation) and the weight of history information w_{k-1} (the second term), through gating unit function. The model can adapt the parameters to environment changes explained as follows: When the first term is zero, current *input* cannot influence current weight of information w_k, indicating that financial environment remains unchanged. On the other hand, when the first term is non-trivial, w_k will change along with the market environment.

From Eq. (5), we process the input by gating unit like Eq. (4), and multiply the input after processing and the weight w_k. The result $input'_k$ is similar to $p_{t+k} * w_k$ in Eq. (3), which can be regarded as the influence at $t + k$ time on prediction.

4. Experiment

4.1. Dataset

We evaluate our model based on the SSCI daily price data sampled from 4th, November, 2009 to 1st, November, 2019. The dataset is retrieved from Yahoo Finance. The data is normalized to range in [0,1], with $p_t = \frac{p_t - \min\_t}{\max\_t - \min\_t}$ (min_t/max_t is the minimum/maximum prize of training data), so that models have faster convergence. We split the whole data into two sections: the training data section is the first 80 percent of data from 4th, November, 2009 to 1st, November, 2017 (total length 1928 days) for training data, and the testing data section is the past 20 percent of data from 2nd, November, 2017 to 1st, November, 2019 (total length 482 days) for testing and model evaluation.

4.2. Experiment Settings

For comparison purpose, we test the performance of other three representative models, i.e., LSTM, CNN, and TABL, except for our model.

The following experimental settings are applied to all network configurations. We choose mean square error (MSE) for loss function, defined as $MSE = \sum_{t=1}^{N} \left(p_t^{real} - p_t^{predict}\right)^2$. Here, p_t^{real} is real price at time *t* and $p_t^{predict}$ is predicted price. As for the evaluation metrics of the model, we consider mean absolute percent error (MAPE), denoted as $MAPE = \sum_{t=1}^{N} \frac{\left|p_t^{real} - p_t^{predict}\right|}{N * p_t^{real}}$, because MAPE measures relative error, which reflects the quality of models accurately.

We adopt Adam optimizer to train the model, in which the learning rate is set to 0.001. Also, Gaussian Distribution is applied to initialize the model parameters. All models are trained for 200 epochs with a minibatch size of 4 samples.

4.3. Experiment Result

For visual comparison, we show the prediction results of different models over the SSCI data in Figure 2. All models perform well in the overall period, with prediction results having the same trend. Nevertheless, in detail, there are transparent deviations from the real prices in the predicted prices from CNN and TABL, while in our model, prediction results fit the real price much better, indicating a better prediction accuracy.

To compare the performance, we calculate MAPE of the models, as in figure 3, the value of daily MAPE changing with time is shown. Each model has different error peak values, which shows that they may learn

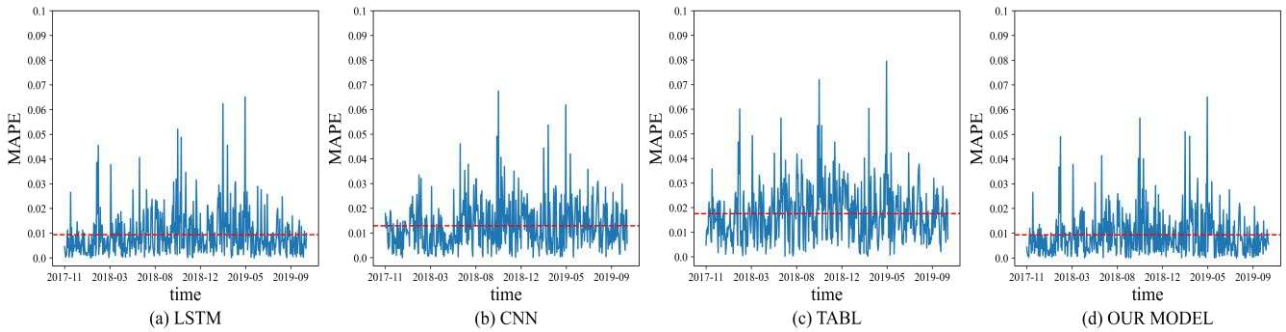


Fig.2 MAPE of different models based on the SSCI.

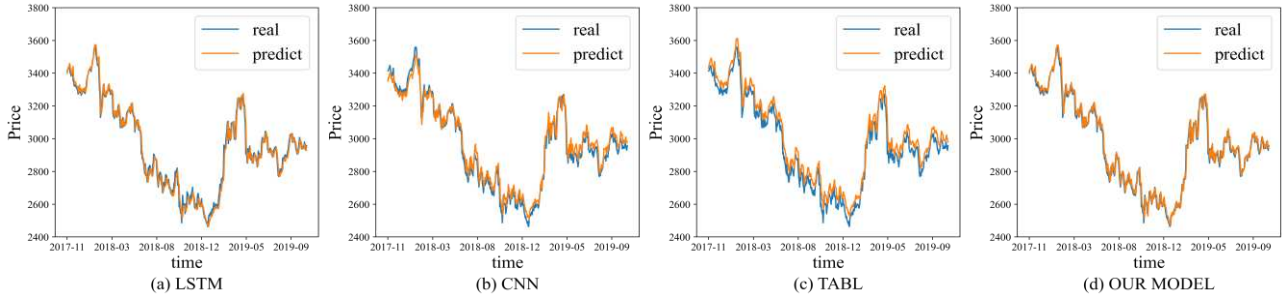


Fig.3 Comperation between prediction result and real price of different models based on the SSCI.

different prediction patterns. Besides, we compare approximate interval of errors. CNN and TABL errors range from 0 to 0.04, LSTM and our model errors range from 0 to 0.02, which means our model can get less error in predictions. Furthermore, we calculate MAPE of the whole testing dataset, which is plotted with red horizontal lines in Figure 3. The MAPE of the whole testing dataset in our model is 0.0124, better than LSTM in 0.0125, CNN in 0.0173 and TABL in 0.0234. The results proves the high effectiveness of our model.

4.4. Hyperparameters Influence

In Table 1, we list two hyperparameters as two main influential factors of the model. One is the length of input times series. We find that when the input length increases from 10 to 20, the error of results decreases, and then increases when the length continues to increase from 20 to 40. The reason is that this hyperparameter characterizes the information capacity, and if the value is low, there is no enough information for prediction, resulting in a high error. On the contrary, when input length is too long, the model may learn some invalid information including noise, leading to increasing prediction error.

The other hyperparameter learned in the model is the RNN cell state dimension, denoting the RNN cell's information capacity. From table 1, the error decreases when the state dimension increase from 10 to 20 but increases when the state dimension increase from 20 to 40. This is because the small value of the state dimension is not able to learn complicated patterns, which is called underfitting. In contrast, the large value of the state dimension will lead to overfitting. Therefore, we should employ appropriate hyperparameters to get more accurate predictions.

Table 1 MAPE for different Hyperparameter setting

Hyperparameters setting		MAPE
Input Length	10	0.0137
	20	**0.0124**
	40	0.0184
RNN cell state dimension	10	0.0178
	20	**0.0124**
	40	0.0197

4.5. Trend Analysis

Though our model can give accurate predictions of daily prices, it is more concerned with long-term information other than everyday fluctuation for those “fundamental” long-term investors. To achieve this, we use Hodrick-Prescott filtering algorithm [21] to predict long-term trend by filtering certain details from our predicted daily prices. The algorithm is optimized by

$$z = argmin\left\{\frac{||t-z||_2^2}{m} + k * \frac{||Dz||_2^2}{m}\right\} \quad (7)$$

where z is the filtered result series, t is our prediction series, m and k is the scaling factor to adjust the filter frequency threshold, and **D** is a filter matrix to filter high frequency. We minimize the 2-norm of vector $||t-z||_2^2$ to ensure the similarity between prediction series and filter results. The minimization of $||Dz||_2^2$ can filter high frequency and get long-term trend results.

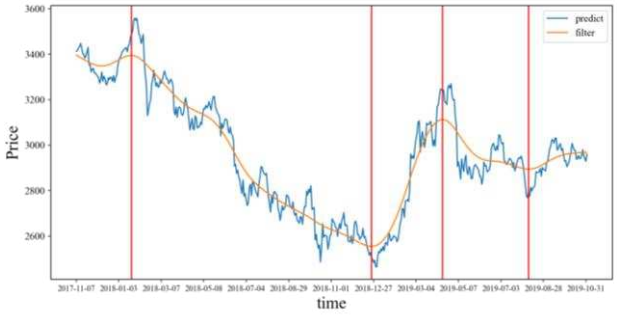


Fig.4 Results using Hodrick-Prescott filtering algorithm.

The results via Hodrick-Prescott filtering algorithm are presented in figure 4. After filtering, there are mainly four periods, corresponding to four tipping points. The first period with descent trend is from January 2018 to December 2018, in which the trade dispute occurred between China and America, with increasing trade tariff, and the economic situation was not clear. The second period is from December 2018 to April 2019, in which the two countries start a series of trade negotiations, reflected in the stock market. The third period is from April 2019 to August 2019, with another decreasing trend, because the relationship froze out again between the US and China. From August 2019 to November 2019, China and the US restarted trade negotiations, and index price trended up. Overall, the index price trend after the H-P filter strongly correlates with the trade war process between China and the US.Besides, there are four tipping points which identify the crash and recovery tipping moments in the SSCI, which gives phase transitions in current financial market systems.

5. Conclusion

In this paper, we build a new model for financial time series prediction. The model uses an RNN structure based on gating units, through which the model can recognize complicated information patterns and adapt to the change in the financial market. The experimental results show that the model gives more accurate prediction compared to other classical models. Moreover, trend analysis and tipping points prediction are also implemented by filtering short-term fluctuations. These results provide a window to risk assessment and portfolio management for the finance industry.

References

[1] K. J. Kim, “Financial time series forecasting using support vector machines” Neurocomputing, Vol 55, No. 1-2, pp.307-319, 2003.

[2] M. Das, S. K. Ghosh, “A probabilistic approach for weather forecast using spatiotemporal inter-relationships among climate variables”, Proceeding of 9th International Conference on Industrial and Information Systems, Gwalior, pp.1-6, 2014.

[3] R. Chandra, M. J. Zhang, “Cooperative coevolution of Elman recurrent neural networks for chaotic time series prediction” Neurocomputing, Vol 86, pp.116-123, 2012.

[4] Y. X. Tian, P. Li, “Predicting short-term traffic flow by long short-term memory recurrent neural network”, Proceeding of IEEE international conference on smart city/SocialCom/SustainCom (SmartCity), pp.153-158, 2015.

[5] G. E. P. Box, G. M. Jenkins, G. C. Reinsel, G. M. Ljung, Time series analysis: forecasting and control, John Wiley & Sons, Hoboken, 2015.

[6] J. Contreras, R. Espinola, F. J. Nogales, et al, “ARIMA models to predict next-day electricity prices”, IEEE transactions on power systems, Vol 18, No. 3, pp.1014-1020, 2003.

[7] E. E. Osuna, Support vector machines: Training and applications, Massachusetts Institute of Technology, 1998.

[8] M. Pal, “Random forest classifier for remote sensing classification”, International Journal of Remote Sensing, Vol 26, No. 1, pp. 217-222, Feb. 2007.

[9] S. Kombrink, T. Mikolov, M. Karafiát, et al, “Recurrent neural network based language model”, Proceeding of Twelfth annual conference of the international speech communication association, pp.2877-2880, 2011.

[10] J. Chung, C. Gulcehre, K. H. Cho, et al, “Empirical evaluation of gated recurrent neural networks on sequence modeling”, arXiv:1412.3555, 2014.

[11] F. A. Gers, J. Schmidhuber, F. Cummins, “Learning to forget: Continual prediction with LSTM”, Proceeding of 9th International Conference on Artificial Neural Networks, pp.850-855, 1999.

[12] C. L. Giles, S. Lawrence, A. C. Tsoi, “Noisy time series prediction using recurrent neural networks and grammatical inference”, Machine learning, Vol 44, pp.161-183, 2001.

[13] K. J. Kim, H. Ahn, “Simultaneous optimization of artificial neural networks for financial forecasting”,

Applied Intelligence, Vol 36, No. 4, pp.887-898, 2011.
[14] L. A. Laboissiere, R. A. S. Fernandes, G. G. Lage, “Maximum and minimum stock price forecasting of Brazilian power distribution companies based on artificial neural networks”, Applied Soft Computing, Vol 35, pp.66-74, 2015.
[15] M. Göçken, M. Özçalıcı, A. Boru, et al, “Integrating metaheuristics and artificial neural networks for improved stock price prediction”, Expert Systems with Applications, Vol 44, pp.320-331, 2016.
[16] J. A. Sirignano, “Deep learning for limit order books”, Quantitative Finance, Vol 19, No. 4, pp.549-570, 2018.
[17] A. Tsantekidis, N. Passalis, A. Tefas, et al, “Forecasting stock prices from the limit order book using convolutional neural networks”, Proceeding of 19th IEEE Conference on Business Informatics, Vol. 1, pp.7-12, 2017.
[18] A. Tsantekidis, N. Passalis, A. Tefas, et al, “Using deep learning to detect price change indications in financial markets”, Proceeding of 25th European Signal Processing Conference, pp.2511-2515, 2017.
[19] W. Bao, J. Yue, Y. L. Rao, “A deep learning framework for financial time series using stacked autoencoders and long-short term memory”, PLoS One, Vol 12, No. 7, pp.1-24, 2017.
[20] D. T. Tran, A. Losifidis, J. Kanniainen, et al, “Temporal attention-augmented bilinear network for financial time-series data analysis”, IEEE transactions on neural networks and learning systems, Vol 30, No. 5, pp.1407-1418, 2018.
[21] S. J. Kim, K. Koh, S. Boyd, D. Gorinevsky, “L1 trend filtering”, SIAM Review, Vol 51, No. 2, pp.339-360, 2009.

A TUNABLE AND EXPLAINABLE ATTRIBUTES (TEA) FOR RECOMMENDATION SYSTEM

MUHAMMAD HASSAN FAROOQ BUTT[1], JIAN PING LI[1], TEHREEM SABOOR[2*]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China
[2]Department of Software Engineering, National University of Computer and Emerging Sciences, Islamabad, Pakistan
E-MAIL: hassaanbutt67@gmail.com, jpli2222@uestc.edu.cn, tehreemsaboor@gmail.com

Abstract:

Recommender system in information retrieval systems recommends relevant items to consumers by inspecting the consumer's preferences and objective behaviours. We received recommendations daily regarding what to take in as food, buy, and choices about the wear trends. However, we can understand our recommendations, and even less, we can tune our preferences efficiently. One main concern is those undesired or irrelevant recommendations, not only wasting our time, but they also cost media companies millions of dollars every year. Considering this issue, we proposed a tunable and explainable recommendation system where the attributes that determined the recommendations are explainable and tunable for every individual consumer. Irrelevant recommendations waste the consumer's time and the company's money, but if we put the power of the recommendations in the consumer's hands, we have a win-win situation. The suggested method addresses recommendation algorithms issues, which creates negative feedback loops and allows consumers to be aware of the profile they are building and tune it to see the content that interests them most.

Keywords:

Recommender System; Information Retrieval; Tunable Preferences; Explainable Recommendations.

1. Introduction

The World Wide Web has brought many variations in the way of our lives. Nowadays, people trust the web and related technologies such as search engines, which look up and take out content and each prospect of life. The data accessibility on the internet allows the user to select from a vast list of products, movies or restaurants, etc. However, these vast choices bear the information cost and their associated cognitive overload on a particular user searching for the most relevant and more reliable Web search information. For addressing these issues, a recommendation system (RS) was developed [1]. RS is the most leading techniques that manage information overloading and advise users with suitable and applicable recommendations [2].

Today, several RS's have been developed for different domains to fulfil the information needs of users. RS aids the user to explore the set of items in a system and find the most relevant items to him/her [3]. The two basic RS categories are the context-based and score-based ones. The first category exploits users' and items' characteristics, while the latter depends on the users' item scores [4]. Traditional implementations of RS are based on TF-IDF and nearest neighbours techniques, while more recent RS follow machine learning (ML) approaches, like matrix factorization and neural networks. ML algorithms' increase in popularity and the "black boxes" of neural networks in deep learning (DL) become the industry standard, pulling out the demographic information, and the user history responsible for each undesired RS becomes next to impossible to achieve.

A genuine issue that comes along with recommendations is whether a user or even the system designer understands the results of the RS. This problem has given rise to the so-called explainable recommendation. Personalized recommendation algorithms for explainable recommendations help in addressing the problem of why [5]. It is not only giving support to system designers or users in terms of recommendation-related results but also clarifies why such a particular product is recommended to him/her. Explainable recommendation helps system designers better debugging of the system and improved transparency, persuasiveness, effectiveness, trustworthiness, and satisfaction for RS [6].

Scientists and researchers have long acknowledged a speed vs. accuracy trade-off in tech fields, but in the recent booming world of artificial intelligence (AI), we are now entering a trade-off between sophisticated models and the interpretability of their predictions. This lack of transparency in RS led us to propose a Tunable and Explainable Attributes (TEA) for the recommender model. In our model, the attributes that determine the recommendations are explainable and tunable to the individual users.

The Paper further has an overview of related literature

discussed in Section 2, including general concepts and techniques based on the explainable RS. Further, Section 3 is on the presentation of the proposed methodology. Whereas Section 4 presents results and findings of experimental work. At last, Section 5 concludes all discussion, also withdrawn future direction and implication.

2. Literature Review

Nowadays, organizations such as YouTube, Amazon, and Netflix, and many other e-commerce-based companies pay great attention to generate high-quality recommendations. Every model or methods have their limitation to some extent. For that purpose, it facilitates the system designer or users with explanations. Explainable recommendations and search attempt to develop the methods or models where explanations can come either directly or indirectly from the explainable model. To the best of our knowledge, some significant overview of the literature is discussed in this section.

Many researchers work on the prediction model and try to improve accuracy. Various methods are proposed to do the same work to help the users to interpret the predictions but often are unclear and not so accurate. Scott et al. [7] addressed the problem and proposed a SHAP (SHapley Additive exPlanations) framework to explain the prediction. They also show improved computation in terms of performance and consistency concerning human notions with that previously proposed approaches.

Nicole et al. [8] give two significant contributions to his proposed work. The first contribution is to provide a unified framework based on polynomials for why-not explanations that consider all databases under probabilistic semantics in a unified manner. His work's second contribution is the algorithm Ted++, which efficiently figure out why-not explanation subordinate with semantics. The main pros achieved by the algorithm is that it significantly reduces time and space consumption. Experimentally proved that the Ted++ algorithm is efficient compared to other existent algorithms and provides useful insights for the developer in its why-not explanation quality.

Zhang et al. [6] presented a comprehensive survey, which is designed in three folds. The first fold of the survey is regarding categorizing the recommendation problem into 5W, i.e., what, when, who, where, and why. The second fold of the survey is regarding three perspectives of explainable recommendation, such as user study approaches and model-based approaches, two-dimensional taxonomy for classification of explainable recommendation, and summarizing the tasks that apply on the explainable as social recommendations. The third fold of the survey is about promoting explainable recommendations by devising the potential future directions.

Shah et al. [4] describe the current hot spots and trends in RS, such as the cold start problem, shilling attacks, and privacy-related issues. He also discussed RS techniques such as content-based, collaborative and hybrid filtering and challenges faced in them like Grey sheep, sparsity, scalability, latency problem, etc. Besides, it also highlights some future research directions to handle these gaps in RS. Afterwards, investigating research opportunities for the high quality and trust-able RS are presented to mitigate these issues.

Azin et al. [9] proposed a mechanism PRINCE (Provider-side Interpretability with Counterfactual Evidence) that is the provider side solution that aimed to detect the actual causes behind the recommendations heterogeneous network of information like with users, items, etc. It is a polynomial-time algorithm because it finds the minimal set of user's actions from the search space in polynomial time. Experimental evaluation is also carried out on two datasets, which shows that PRINCE gives more compact explanations concerning intuitive baseline.

Brian et al. [10] describe a controlled study comparing the four questions design in why, why not, how-to, and what if. In this regard, they developed the web-based I/O interface as intelligent prototypes with different explanations. The experimental evaluation shows that by providing the trace explanation and Why explanation to the novice, the user can improve the user's trust and understanding in the system.

Yongfeng et al. [5] work based on explainable recommendations, improved system trust, effectiveness, and transparency. The focus is on search algorithms and their application in real-world systems like e-commerce, social networks, etc., for explainable recommendations.

3. Proposed Methodology

We start our proposed methodology by providing an example of understanding a typical movie RS pipeline with a user having the name Lee. Lee has a list of personal attributes and a set of criteria for his movie recommendations.

To address the cold start problem, we will assume Lee is a new user and will generate recommendations for him without knowing his past movie ratings. For this particular case, match Lee with similar users and then make movie recommendations for Lee based on their movie ratings.

Once Lee has entered some characteristics about himself (male, engineer, age 30, from CA) and some movie preferences (genres: action and adventure, minimum average movie rating: 3-star, and the number of movies to be recommended: 3 movies), Using these factors and a cosine similarity function using Equation (1), ETA generates the

following three movies for Lee: (Indiana Jones, Star Wars, and Star Wars) as a return.

$$Similarity\ (p,q) = cos\emptyset = \frac{p.q}{||p||||q||} = \frac{\sum_{i=1}^{n} p_i q_i}{\sqrt{\sum_{i=1}^{n} p_i^2}\sqrt{\sum_{i=1}^{n} q_i^2}} \quad (1)$$

Since we are interesting to calculate the cosine similarity for two vector and their expected output. The output always ranges from -1 to 1. The output 1 means that two items are similar whereas output -1 means that two items are dissimilar to each other. So here we used the cosine similarity in context to know how the movies are similar to each other.

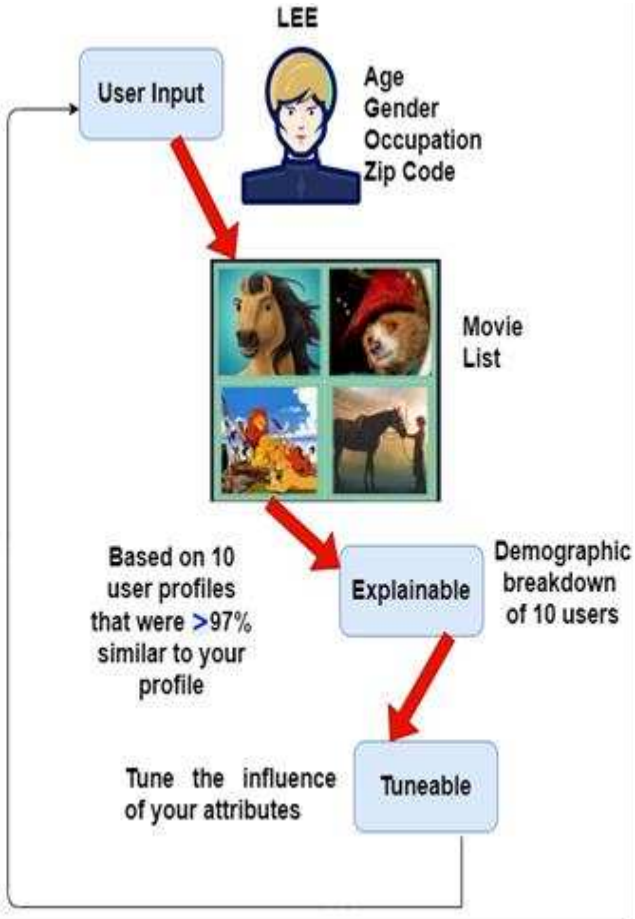


Fig.1 Proposed Approach of TEA

Lee is made aware that his movie recommendations are determined from the 10 (default) most similar user profiles to his own, where the average similarity is 98%. The number of most similar users, in this case, is a tunable factor. Increasing the number of similar user profiles can generate a more diverse set of movies but might result in movies, Lee would be less interested in.

Lee is also led into the attribute breakdowns of those ten most similar user-profiles and can draw his conclusions about the impact his attributes have on his recommendations. For example, all the movies recommended to Lee were rated by male users, and 6 of the ten most similar user profiles had a technical profession. Lee may be satisfied with these numbers and will move on to enjoy his movie night, or he may choose to customize his recommendations further.

So, any user can scale the importance of each of their attributes from 0–100. So, if Lee's most important factor in determining his movie recommendations is occupation, he must weigh that attribute relatively higher than the rest of his attributes. After Lee scaled his engineering occupation as the highest attribute, his movie recommendations shifted to Sci-Fi! as shown in figure 1.

We also needed to figure out a way to best match Lee with similar users to provide movie recommendations. The problem with one-hot encoding is that each attribute vector is equidistant from every other attribute vector.

While this is fine for continuous values like age, which fall on a continuous scale and are easy to normalize, one-hot encoding is not ideal for categorical data like occupation because some occupations are more similar than others.

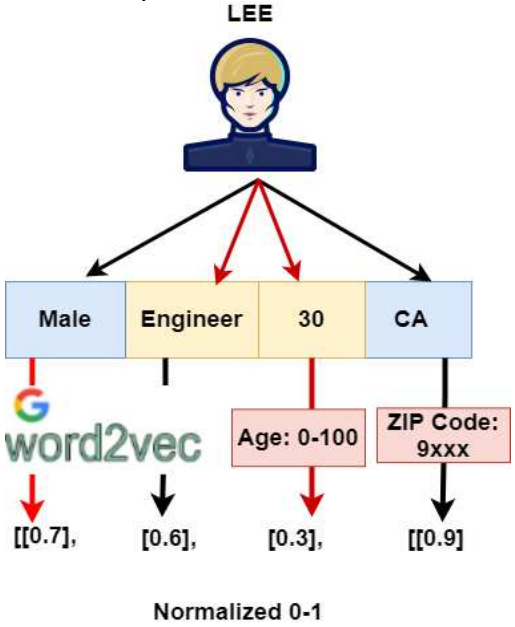


Fig.2 User-Attribute Vector

As shown in figure 2, an engineer might have more movies in common with a technician than an entertainer. For this reason, after taking the user profiles that have a similarity score to Lee higher than .7, we used Google's word2vec and the distance to a given word to vectorize specific attributes. We chose to do this for occupation and gender but would like to extend the future to more non-binary attributes. We again used a cosine similarity function to find the ten most similar users to Lee.

4. Experimental Analysis

This section covered the experimental analysis that is performed on the real-world dataset and reports the results accordingly.

4.1. Datasets

Since the usefulness of CF models is dependent on how large and robust your dataset is, we used the MovieLens [11] Dataset complete with 100K movie ratings, 1,682 movies, and 943 users (with the same latent attributes as Tom). Movielens provides 1M/10M/20M datasets for a larger variety of recent movies (but use with caution as the file structure may have changed).

To evaluate of our proposed method in terms of better performance, we divide under consider data set into 10 parts comprises of test and training dataset, whereas 1 part comprises of test sets and remaining 9 part are in training sets. So by this we get an average of 10 test as final results from experimentation.

4.2. Evaluation Metric

Mean absolute Error (MAE) and Root Mean Square Error (RMSE) are the two evaluation metric which is used to assess the predictive accuracy related to ratings that are generated by the recommendation system. As the predictive accuracy is higher, when smaller their values are, we get the better performance as a result. The Evaluation metric are shown below in Equation (2) and (3).

$$MAE = \frac{1}{N_{DS}} \sum_{(u_i,p_j)\in DS} |\hat{r}_{u_i p_j} - r_{u_i p_j}| \quad (2)$$

$$RMAE = \sqrt{\frac{1}{N_{DS}} \sum_{(u_i,p_i)\in DS} (\hat{r}_{u_i p_j} - r_{u_i p_j})^2} \quad (3)$$

Where $r_{u_i p_j}$ is the actual ratings of item p_j from $u_{I,}$ $\hat{r}_{u_i p_j}$ is its predicted rating, and N_{DS} is the total number of items in the test dataset DS.

Table 1 MAE and RMSE Results Comparision

Methods	Mean Average Error (MAE)	Root Mean Average Error (RMAE)
Sklearn-k-means	0.748	0.969
Sklearn-k-NN	0.733	0.942
Skleran-SVD	0.737	0.925
Keras-MF (TEA)	0.693	0.894

We used Keras to solve matrix factorization and it has been outperforming other ML algorithms for predicting ratings as shown in table 1.

4.3. Results Discussion

It is a reality; we probably exit the movie as soon as it ends without submitting a rating. As you might suspect, this leads to a very sparse user-movie matrix (only 7% of the entries are filled). We have to address the sparsity problem before we can give movie recommendations to Lee. Moreover, since some users consistently rate movies conservatively (1–2 stars), while other users are more generous with their movie ratings (4–5 stars), we need to normalize all user's movie ratings to average three stars.

Next, we use low-dimensional representations to predict user ratings for unseen movies. This is done by decomposing a high dimensional matrix into two lower-dimensional matrices using Keras. Matrix factorization in Keras with an Adam optimizer is used because it outperforms other machine learning algorithms for predicting ratings (Mean Average Error = 0.693). Not only does this address the sparsity issue but, by using matrix factorization, we increase the likelihood of excellent but not well-known movies being recommended.

Now, when Lee gets his movie recommendations, he has options for explainability and adjustability. Lee not only can see why these particular movies were recommended to him, but he can also tune his attributes to align with his preferences.

Another exciting result occurs after changing Lee's gender to female and scaling it to 100 while scaling the three other attributes to 0. This changes Lee's top Action & Adventure recommendations from Die Hard to Titanic. What we see from this is the bias present in movie recommendations. However, what comes first, the click or the recommendation? While this chicken or egg scenario is still up for debate, identifying a way to reduce that bias by tuning the factor directly related to the recommendation is a step in the right direction for putting ad control back in consumers' hands.

5. Conclusions

While RS's consider many more than four attributes and the user history and are much more complicated than this method, this concept shows that each ad recommendation we receive on media sites can be understood. Neither companies nor consumers benefit from users clearing their history due to irrelevant ads. With the right combination of models and tools, we will adjust our preferences transparently across multiple platforms, and we can finally be rid of the mermaid movies. The innovation of this method in contrast to other advanced RS's is that our method provides recommendations to users with explanations on why they are getting these

movies as recommendation. Also, it gives power to the users to tune their preferences according to their interest and get more personalized recommendations. This method can be applied in real applications such as Netflix, Amazon Prime and other movies RS platforms.

In future, we aim to explore Why-Not, machine learning-based explainable recommenders. In a second phase, we aim to extend the recommenders so that they can leverage the Why-Not explanations for auto-tuning.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, the project of Science and Technology Department of Chongqing Municipality, Chengdu Chengdian Network Technology Co., Ltd., Chengdu Civil-military Integration Project Management Co., Ltd., and Sichuan Yin Ten Gu Technology Co., Ltd.

References

[1] Pu, Pearl, Li Chen, and Rong Hu. "Evaluating recommender systems from the user's perspective: a survey of the state of the art." User Modeling and User-Adapted Interaction, Vol. 22, No. 4-5, pp. 317-355, October 2012.

[2] Khusro, Shah, Zafar Ali, and Irfan Ullah. "Recommender systems: issues, challenges, and research opportunities." In Information Science and Applications (ICISA) 2016, pp. 1179-1189. Springer, Singapore, February 2016.

[3] Francesco Ricci, Lior Rokach, and Bracha Shapira, "Recommender systems: introduction and challenges," In Recommender systems handbook, pp. 1–34, April 2015.

[4] Jiang, Liaoliang, "A trust-based collaborative filtering algorithm for E-commerce recommendation system", Journal of Ambient Intelligence and Humanized Computing, Vol 10, No. 8, pp. 3023-3034, August 2019.

[5] Zhang, Yongfeng, Guokun Lai, Min Zhang, Yi Zhang, Yiqun Liu, and Shaoping Ma. "Explicit factor models for an explainable recommendation based on phrase-level sentiment analysis." In Proceedings of the 37th international ACM SIGIR conference on Research & development in information retrieval, pp. 83-92, July 2014.

[6] Zhang, Yongfeng, and Xu Chen. "Explainable recommendation: A survey and new perspectives." arXiv preprint arXiv:1804.11192, April 2018.

[7] Lundberg, Scott M., and Su In Lee. 2017. "A Unified Approach to Interpreting Model Predictions." Advances in Neural Information Processing Systems (Section 2): pp. 4766–75, December 2017.

[8] Bidoit, Nicole, Melanie Herschel, and Aikaterini Tzompanaki. "Efficient computation of polynomial explanations of why-not questions." In Proceedings of the 24th ACM International on Conference on Information and Knowledge Management, pp. 713-722, October 2015.

[9] Ghazimatin, Azin, Oana Balalau, Rishiraj Saha Roy, and Gerhard Weikum. 2020. "Prince: Provider-Side Interpretability with Counterfactual Explanations in Recommender Systems." WSDM 2020 - Proceedings of the 13th International Conference on Web Search and Data Mining, pp.196–204 January 2020.

[10] Lim, Brian Y., Anind K. Dey, and Daniel Avrahami. 2009. "Why and Why Not Explanations Improve the Intelligibility of Context-Aware Intelligent Systems." Conference on Human Factors in Computing Systems - Proceedings, pp. 2119-2128, April 2009.

[11] https://grouplens.org/datasets/movielens/

AN OPINION AND CONTEXT-AWARE INVERTED INDEX GRAPH MODEL FOR SENTIMENT SEARCH AND ANALYSIS

KPIEBAAREH MICHAEL[1], WU WEI-PING[1], ZHOU HONGTAO[1], WU CHENGCHENG[1], TANG YUQI[1]

[1]School of computer science and engineering, University of Electronic Science and Technology of China, China
E-MAIL:kpiebaareh@yahoo.com, wie-ping.wu@sipingsoft.com, hongtao.zhou@sipingsoft.com, chengcheng.wu@sipingsoft.com, yuqi.tang@sipingsoft.com

Abstract:

Two major functions required in textual data modelling and knowledge discovery especially in modern customer interaction and research are search and sentiment analysis. Recent research has however not been able to combine these two in a way that instils flexibility into the iterative process of textual analysis for decision making. In this work, the Opinion and Context-Aware Inverted Index graph model is proposed for performing sentiment search and analysis on textual data. Unlike previous works, the use of the proposed model retrieves needed information without requiring re-processing of sentiment information. The proposed approach clarifies the difference between sentiment search and sentiment categorization. Furthermore, it shows how to perform opinion aware search based on graph traversals, pattern matching and aspect opinion filtering. To evaluate the flexibility and capabilities of the proposed scheme, the feature interest range, customer feature satisfaction/dissatisfaction intensity, feature co-mentions, and sentiment based ranking metrics of various bipartite projections for feature co-mention sub graphs using PageRank are extracted from a well-studied dataset on online product reviews with an extension of the proposed model. The chosen design and methodology is shown to be suitable for big data scale implementations.

Keywords:

Information Search and Retrieval; Opinion mining; Online product reviews; Labelled property graph; Graph database

1. Introduction

Due to phenomena like electronic commerce, increased competition, and shorter product lifecycles, traditional techniques used by product and service developers to establish a high-quality information channel between themselves and their customers no longer suffice. Such techniques include in-person interviews, focus groups, and observation of the products in use [4]. These activities are expensive, heavily dependent on direct interaction with customers, and are often slow. For instance, a typical interview in the product design industry is about one to two hours long [4]. Product and service designers are now more inclined to pursue digital engagement with customers and products. Techniques like natural language processing and opinion mining are employed to process the resulting data in support of decision making. With some proposed opinion mining schemes displaying high-performance metrics [3], it is only natural that there should be a corresponding and related body of research into the democratization of the results of these techniques. The collection of raw data from customers and the interpretation of this data according to the needs of the customers are two important steps of the process of identifying customer needs [4].

Whiles the source, format, and size of data have changed, the intrinsic goals for processing the information within have not. A reliable form of representation of customer data as a digital knowledge base and the subsequent seamless interaction for search and analysis remains a reigning business goal.

Whiles significant effort has been invested in extracting product and service aspects and opinions polarities from documents [1], not much consideration has been given to providing functionality for using the results. Akin to search engines and recommender systems, opinion mining initiatives work mainly to reduce the information overload faced by decision-makers. Contrary to these technologies, opinion mining solutions are neither widely available nor user friendly for the non-technical decision-makers. Product and service users, designers and researchers stand to benefit from intuitive and flexible opinion-aware aspect-based search and analysis on review data.

In this work, a brief definition of sentiment search is given and contrasted with sentiment categorization or classification. A Label Property Graph-based opinion-aware inverted file model for aspect-sentiment search is proposed for performing sentiment search. An extension of this model that achieves semantic and context-based functionalities is proposed and applied to the product design domain. This

work shows how to perform opinion aware search based on graph traversals, pattern matching and aspect opinion filtering.

2. Related work

Most of the works that attempt to deliver on providing the function of sentiment search take a somewhat counterintuitive approach. As explained earlier, the primary reason why the effort expended in building huge indexes like those used for the World Wide Web is that the gains in the utilization of the resulting index are great. Using the concept of sentiment queries from users and standard inverted indexed documents stored in Oracle Text, [13] pursues the goal of sentiment aware queries. Based on a two-part query (a lexical query component and a sentiment query component), matching documents are first extracted and then sentiment classifications are generated for the retrieved data. For sentiment-based search in a big data scenario, the user will have to wait for this computation to complete for each query thereby affecting the user experience.

In the sentiment search scheme proposed by [5], online reviews are classified according to the overall sentiment expressed on them. Although different from topical categorization [10] which groups web search results according to topics, the technique still lacks the feature to engage search at the sentence or word level. Users typically search by keywords or key phrases and without the knowledge of the sentiment polarity of those keywords, it is impossible to tell which exact documents/reviews satisfy the information need. The work in [7] follows a similar pattern by performing sentiment categorization of web search results. Deployment sentiment analysers are not instantaneous, and depending on the size of data and choice of algorithm, it will be counterproductive for a user to wait for computation and subsequent filtering of search results into positive, negative and neutral before final results are made available. A knowledge graph-based approach was used in similar entity search in [11]. The search was done at the entity level and did not consider complete retrieval of documents based on the sentiment score they expressed on existing entities.

The proposed sentiment management framework in [18] allows for filtering of sentences by the topics of an input entity. The challenge is this case is that users have no control over which keywords should be the focus of the sentiment analysis as they are determined by the number of topics are produced by an LDA technique. LDA methods tend to leave out non-noun aspect terms with these errors propagating deep into the extraction phase. There is also the tendency of keywords in various topics to intersect in LDA techniques and so results may not be as clean as those of targeted keyword search. Extra techniques are often required to mitigate such fallouts [1]. Furthermore, as sentiment categorization is not used as a pre-processing task in [18], the user needs to wait for the computation of sentiments once the target sentences are identified.

3. A proposed method for sentiment-based search (sentiment search)

Based on the traditional inverted index, the concept of information retrieval is explained as follows; users have information needs which they expect to find in documents. These needs and the documents have their respective representations (query representation and document representation) based upon which a system tries to ascertain how well a document or set of documents satisfies the information need [9]. The primary feature of search engines and information retrieval systems, in general, is their ability to index documents and evaluate queries [12]. In the sections that follow, the detail of how to achieve sentiment search to match the sentiment needs of users to documents is provided.

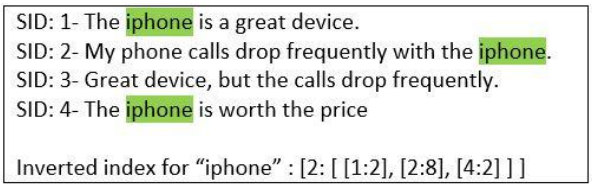


Fig.1 Representation of an inverted index

3.1. Sentiment search

We define sentiment search as an Information Retrieval (IR) task for which an appropriate data model enables the sentiment polarity of the key document tokens to form an essential part of the metadata of a document indexing scheme. This means that most of the processing related to the document representation is approached as a pre-processing task. This task includes the sentiment categorization and indexing of tokens. This makes the search activity launched by a user fast and user friendly.

Fig.1 shows the extraction of the inverted index of the “iphone” token in a corpus of four (4) sentences. At a high level, metadata captured are the sentence IDs and a collection of token-sentence ID pairs for all occurrences of the token in the corpus sentences. Besides the total occurrences, other metadata can be captured as well. This basic concept is modified in a flexible way to achieve the goals of this paper in the following sections.

3.1.1. Document representation: Opinion and Context-Aware Inverted Index (OCAII) graph data model

In this work, we propose the Opinion and Context-Aware Inverted Index (OCAII) graph data model. It is based on a labelled property graph and allows the search of a corpus by using specific keywords and a further filter based on the sentiment polarity expressed on the keywords. This is especially useful for conducting aspect-based sentiment analysis in customer reviews analysis. Neo4j graph database is used because it is a native labelled property graph capable of supporting our model, performing full-text search (inverted index) and handling millions of nodes and a billion relationships on a Big Data scale[14][15]. In a property graph, both the edges and their constituent vertices can have properties assigned. The resulting construct, a multi-relational property graph, presents enough flexibility to expediently model complex domains into efficient, searchable spaces [17].

Fig.2 illustrates the Labelled Property Graph model of an inverted index graph model for the same index structure in **Fig.1**. With the flexibility of this data structure, it becomes possible to attain a context richer index by defining the relationship between tokens and sentences with token positions, sentiment polarity/scores, and the Part Of Speech properties.

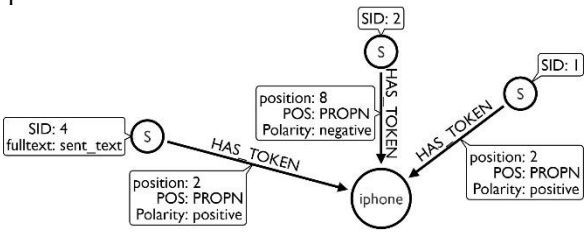


Fig.2 Opinion and Context-Aware Inverted Index graph model view with arrows incoming to the token node to signify that sentences have semantic and sentiment influence on it.

By taking a reverse view (**Fig.3**) from the OCAII graph model, all token nodes and their properties can be reached from a given sentence node for extraction or modification. **Figure.4** enumerates the steps needed to generate a standard dataset that can support this graph model.

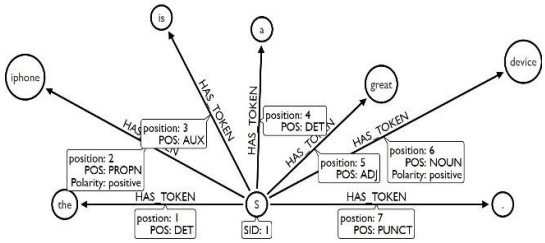


Fig.3 Reverse OCAII graph model view showing the reach of a sentence node and sentiment relationships with tokens.

Algorithm 1: Algorithm for generating a data set for a labeled Property Graph-based inverted index model

```
/* Part of Speech (POS)                                          */
Input: Reviews
1  foreach reviewinReviews do
       /* Clean and split Reviews into sentences                 */
2      sentences = Preprocess(review)
3      foreach sentinsentences do
4          sent_no= sent_no + 1
5          sent_no=0
6          for token ∈ sent do
7              token_position=token_position + 1
8              row = [sent_no,token_position,token.text,
                token.POS ]
9              GraphSet <--append-- row
Output: GraphSet
```

Figure.4 Algorithm for generating the OCAII graph dataset.

3.1.2. Aspect based sentiment analysis: classification / annotation / categorization

This step can be handled by either machine learning methods or by using a human annotator as a pre-processing step. Based on the tags assigned to tokens and word phrases in the preceding steps (**Fig.5**), the sentiments of select (target) tokens (nouns) are computed using three algorithms to capture the sentiment strength from various perspectives on line 12. Firstly, an algorithm which leverages the proximity of opinion words to target words is used to compute the sentiment score on these targets.

The second algorithm is based on the segmentation of sentences into parts separated by comparison words ([***but, however, albeit, although, in contrast, despite, though, on one hand, on the other hand, then again, even so, unlike, while, conversely, nevertheless, nonetheless, notwithstanding, yet***]). The sentiment of the word is then solely produced based on the segment of the sentence where it is located. Thirdly, the semantic dependencies accessed

through natural language dependency parsing is used to score the sentiments of target tokens. Opinion bearing words are naturally close to targets (nouns) when dependency parsing is applied [16]. All three scores are then aggregated by an aggregation function to get the final sentiment score which is used as an aspect sentiment polarity tag.

Algorithm 2: Algorithm for enriching tokens with selected tags with sentiment scores

```
/* List of target tags (TTAGS)                                   */
Input: TTAGS
aspect_tokens=[]
token_position=0
if token.tag ∈ TTAGS then
    aspect_tokens ←append— token
foreach token ∈ aspect_tokens do
    /* Q1                                                        */
    sentence_ids = get_distinct_sentence_ids(token)
    foreach sent_id ∈ sentence_ids do
        /* Q2                                                    */
        sent_text= get_sorted_tokens ({sent_id},
          HAS_TOKEN, token)
        sentence=""
        for text ∈ sent_text do
            sentence = sentence + " " + text
        /* Use Algorithm 3 to compute sentiment score            */
        polarity = compiled_sentiment(sentence,token)
        set_polarity(sent_id,
          HAS_TOKEN{Polarity:polarity}, token)
Output: GraphSet
```

Fig.5 Algorithm for enriching tokens with selected tags with sentiment scores.

4. Application of the proposed graph model: product design aspect-based opinion search and analysis on customer reviews

With graph traversal, pattern matching and property filtering, it is possible to reach any connected part of a large labelled property graph. The SemEval-2014 dataused for evaluating the proposed approach comprises more than 3000 sentences extracted from customer reviews of laptops. Two annotations (aspect term, polarity(negative, positive, neutral, conflict)) have been provided by experienced human annotators. The base OCAII graph model (**Fig.2**) is enriched (**Fig.6**) with the HAS_ASPECT edge, assigned sentiment property and connected to its aspect term node.

Adopting the notation in [17][19], the traversal of equation (1) starts at a given token node t, follows its incoming edge, includes (lab+) the edge on the path if it has the HAS_TOKEN label and then includes the polarity property from it. Equation (2) follows a similar path but extends further to extract the sentence ID of the sentence node at the end of the path. A typical use case for equation (3) is token extraction and sorting according to the token position number, the whole sentence can be assembled and extracted.

$$g_1 = (\epsilon_{p+}^{polarity} \circ e_{lab+}^{HAS\_TOKEN} \circ e_{in})(\mathrm{t}) \quad (1)$$

$$g_2 = (\epsilon_{p+}^{sentence\_no} \circ v_{out} \circ e_{lab+}^{HAS\_TOKEN} \circ e_{in})(\mathrm{t}) \quad (2)$$

$$g_3 = (\epsilon_{p+}^{token} \circ v_{in} \circ e_{lab+}^{HAS\_TOKEN} \circ e_{out})(\mathrm{s}) \quad (3)$$

Token extraction can also be achieved with fine-grained filtering to extract by sentiment score or POS tag (e.g. all of the instances of "google" as a verb). A version of equation (3) traversing the HAS_APSECT edge is used to extract a count of aspect terms of interest to reviewers and displayed in **Fig.7** Customer interest range distribution (top 20 aspect terms). Two similar traversals are executed to compute the in-degree on the top 10 results in **Fig.8**, one for positive sentiments and another of negative sentiments.

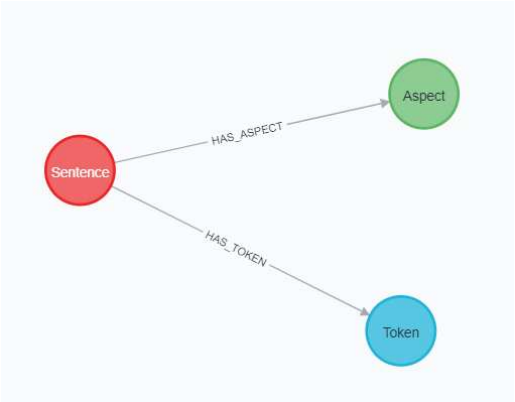


Fig.6 Schema for extended OCAII graph model for product design analysis

$$g_4 = (\epsilon_{p+}^{token<>a\ and\ token.polarity<0} \circ v_{in} \circ e_{lab+}^{HAS\_TOKEN} \circ e_{out} \circ S_{out} \circ e_{lab+}^{HAS\_ASPECT} \circ e_{in})(\mathrm{a}) \quad (4)$$

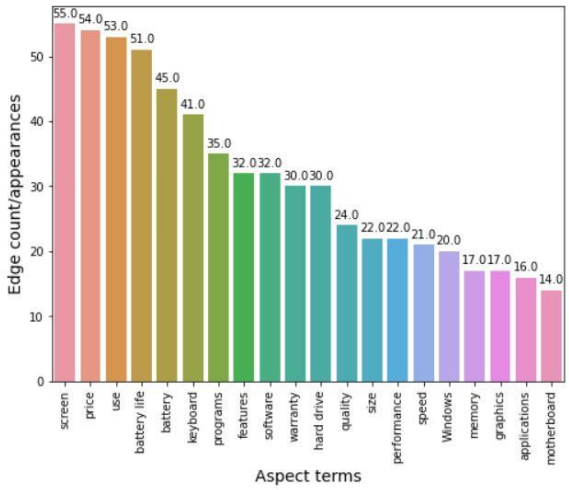


Fig.7 Customer interest range distribution (top 20 aspect terms)

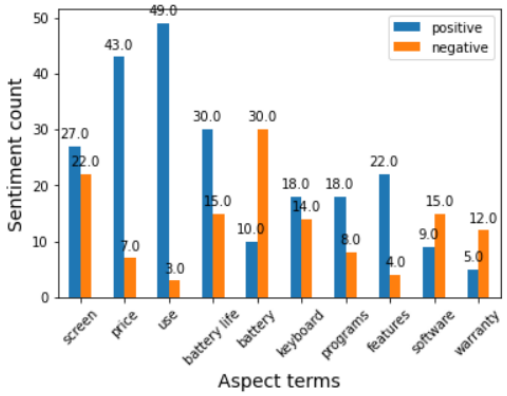


Fig.8 Customer feature satisfaction/dissatisfaction intensity distribution (top 10 aspect terms)

From **Fig.7**, it is observed that "***battery***" aspect term is ranked 5th in total edge in-degree after "***battery life***" but has the highest dissatisfaction rank in **Fig.8**. The traversal pattern in equation (4) is generated to perform sentiment search on all co-negative tokens mentioned in sentences where the "***battery***" aspect term is found. In addition to battery complaints, the set of tokens **{'netbook': 1, 'repair': 1, 'side': 1, 'software': 1, 'mac': 1, 'lot': 1, 'iwork': 1, 'downfall': 1, 'macconnection': 1, 'research': 1, 'rate': 1}** also have negative sentiments on them. We go further to generate more sentiment search metrics for "***battery life***" term, "***battery***" token and "***life***" token to gain clarity on their relationships. The counts for tokens are structured as [total count, negative count, positive count] as follows; "***battery***" aspect term [45,30-,10+, 1 conflict, 1 neutral], "***battery life***" aspect term [51,15-,30+, 3 neutral, 3 conflict] and for "***battery***" token [101,18-,83+]. Out curiosity to find combinations of "***batter***" & "***life***" tokens, we found 7 sentences. Ordering the position IDs for the "***battery***" and "***life***" tokens gave us ([2,3], [16,17], [10,11] ,[**6,14**], [12,13], [9,10],[2,3]) showing that "***batter life***" was used explicitly in all but one sentence.

This shows clearly that most of the opinions (negative in context) on "***battery life***" were made implicitly by reviewers whiles explicit "***battery***" opinions were generally positive.

The top 5 results of applying PageRank to top 10 sub graph of aspect terms are; {**'battery life': 0.1644**, 'screen': 0.1439, 'use': 0.1422, 'price': 0.1233, 'features': 0.1158}. For Page rank of the co-mentions sub graph over all (+, -, neutral) aspects and sentiments; {**'keyboard': 0.0177**, 'screen': 0.0144, 'battery life': 0.0114, 'software': 0.0113, 'hard drive': 0.0111}, and for Page rank over co-negative sub graph of top 10 aspects {**'battery life': 0.1919**, 'keyboard': 0.1, 'screen': 0.1, 'software': 0.1, 'price': 0.1}. Interestingly, "**battery**" aspect is not as dominant in the real ranking metrics.

5. Conclusions

Much needed solutions for sentiment search have not been pursued and given much attention by recent research. The consumers of sentiment analysis in positions of decision making within organizations require flexible and intuitive solutions to understand customer sentiment without waiting for NLP pipelines to be executed after each query. In this paper, we proposed the OCAII graph model and applied it to the field of product design to analyse user sentiment on Laptops. We show that once the model is built, it becomes a trivial task to access sentences containing specific tokens or aspect terms based on specific sentiment polarity orientation. The solution was easily extended to extract the user feature interest range, feature satisfaction/dissatisfaction intensity and co-negative feature mentions in a product reviews analysis. By leveraging bipartite co-mentions sub graph networks (using co-mention counts as edge weights), sentiment based aspect ranking was performed by filtering the edges according to sentiment polarity. The proposed graph model supports sentiment search since it indexes every token along with its position in a sentence, its POS tag and its sentiment within the sentence.

The flexibility of the approach stimulates further research and so in future work, we intend to expand the size and richness of context in the space of search engines and knowledge graphs for aspect-based opinion mining.

References

[1] Wang, Rui, Deyu Zhou, Mingmin Jiang, Jiasheng Si, and Yang Yang. "A survey on opinion mining: From

stance to product aspect." IEEE Access 7 (2019): 41101-41124.
[2] Hemmatian, Fatemeh, and Mohammad Karim Sohrabi. "A survey on classification techniques for opinion mining and sentiment analysis." Artificial Intelligence Review (2019): 1-51.
[3] Sindhu, Irum, Sher Muhammad Daudpota, Kamal Badar, Maheen Bakhtyar, Junaid Baber, and Mohammad Nurunnabi. "Aspect-based opinion mining on student's feedback for faculty teaching performance evaluation." IEEE Access 7 (2019): 108729-108741.
[4] Eppinger, Steven, and Karl Ulrich. Product design and development. McGraw-Hill Higher Education, 2015.
[5] Al-Obeidat, Feras, Bruce Spencer, and Eleanna Kafeza. "The opinion management framework: Identifying and addressing customer concerns extracted from online product reviews." Electronic Commerce Research and Applications 27 (2018): 52-64.
[6] Khoo, Christopher SG, Norraihan Bte Hamzah, Syin Chan, and Jin-cheon Na. "Sentiment-based search in digital libraries." In Proceedings of the 5th ACM/IEEE-CS Joint Conference on Digital Libraries (JCDL'05), pp. 143-144. IEEE, 2005.
[7] Na, J.-C., Khoo, C., & Chan, S. (2006). A sentiment-based meta search engine. In C. Khoo, D. Singh & A.S. Chaudhry (Eds.), Proceedings of the Asia-Pacific Conference on Library & Information Education & Practice 2006 (A-LIEP 2006), Singapore, 3-6 April 2006 (pp. 83-89).
[8] Uddin, Gias, and Foutse Khomh. "Opiner: an opinion search and summarization engine for APIs." In 2017 32nd IEEE/ACM International Conference on Automated Software Engineering (ASE), pp. 978-983. IEEE, 2017.
[9] Manning, Christopher D., Hinrich Schütze, and Prabhakar Raghavan. Introduction to information retrieval. Cambridge university press, 2008.
[10] Zeng, H.-J., He, Q.-C., Chen, Z., Ma, W.-Y., and Ma, J. Learning to Cluster Web Search Results, In Proceedings of the 27th Annual International ACM SIGIR Conference, Sheffield, South Yorkshire, UK, July 2004, 210-217.
[11] Metzger, Steffen, Ralf Schenkel, and Marcin Sydow. "Aspect-based similar entity search in semantic knowledge graphs with diversity-awareness and relaxation." In 2014 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT), vol. 1, pp. 60-69. IEEE, 2014.
[12] Sharma, Sunny, Sunita Mahajan, and Vijay Rana. "A semantic framework for ecommerce search engine optimization." International Journal of Information Technology 11, no. 1 (2019): 31-36.
[13] Roy, Shubhro Jyoti, Alexandra Czarlinska, and Asha Tarachandani. "Framework for Sentiment Aware Queries and Results in Search Using Oracle Text." International Journal of Knowledge Engineering 1, no. 2 (2015): 84-85.
[14] Aung, Thet Thet, and Thi Thi Soe Nyunt. "Community Detection in Scientific Co-Authorship Networks using Neo4j." In 2020 IEEE Conference on Computer Applications (ICCA), pp. 1-6. IEEE, 2020.
[15] Needham, Mark, and Amy E. Hodler. Graph Algorithms: Practical Examples in Apache Spark and Neo4j. O'Reilly Media, 2019.
[16] Kübler, Sandra, Ryan McDonald, and Joakim Nivre. "Dependency parsing." Synthesis lectures on human language technologies 1, no. 1 (2009): 1-127.
[17] Rodriguez, Marko A., and Peter Neubauer. "The graph traversal pattern." In Graph Data Management: Techniques and Applications, pp. 29-46. IGI Global, 2012.
[18] Al-Obeidat, Feras, Bruce Spencer, and Eleanna Kafeza. "The opinion management framework: Identifying and addressing customer concerns extracted from online product reviews." Electronic Commerce Research and Applications 27 (2018): 52-64.
[19] Kpiebaareh, Michael Y., Wei-Ping Wu, Strato Bayitaa, Charles R. Haruna, and Lawrence Tandoh. "User-connection behaviour analysis in service management using bipartite labelled property graph." In Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pp. 318-327. 2019.

RECOMMENDATION OF SIMILAR LANDSLIDE CASES BASED ON LANDSLIDE PROFILE

LEI-YU DAI[1], MING-CANG ZHU[2], ZHI-GANG MA[3], ZHAN-YONG HE[3], HONG JIANG[3], PENG-SHAN LI[4], XIAO-BO ZHANG[5], JI-BAO SHI[5], KAI CHEN[5], TAO WENG[5], ZE-ZHONG ZHENG[1]*, QIANG LIU[1]*

[1]School of Resources and Environment, University of Electronic Science and Technology of China, Chengdu, Sichuan, PRC 611731
[2]Department of Natural Resources of Sichuan Province, Chengdu, Sichuan, PRC 610072
[3]Sichuan Research Institute for Eco-System Restoration & Geo-disaster Prevention, Chengdu, Sichuan, PRC 610081
[4]Chengdu Land Planning and Cadastre Center, Chengdu, Sichuan, PRC 610074
[5]Chengdu Institute of Survey & Investigation, Chengdu, Sichuan, PRC 610081
E-MAIL: zezhongzheng@uestc.edu.cn.

Abstract:

In landslide disaster prevention project, landslide profile is an important research object, which contains rich geological information of landslide. When we get the profile image of the landslide, if we can recommend several landslide cases with similar geological characteristics by the landslide profile image for research, the landslide disaster prevention project can be carried out quickly. In this paper, we propose a recommendation system based on similarity of landslide geological characteristics. The recommendation system is divided into two steps. Firstly, we construct a classification model to obtain the categories of landslide geological characteristics from the profile image by random forest algorithm and supervised machine learning approach. Then, according to the categories of landslide geological characteristics, the landslide case recommended model is constructed, and 5 landslide cases with similar geological characteristics are recommended for the landslide. According to the evaluation index of the recommendation system, the evaluation results show the effectiveness of the recommendation system.

Keywords:

Landslide; Landslide disaster prevention project; Image classification; Profile; Recommendation system.

1. Introduction

In the field of landslide disaster prevention project, if refer to the research results of landslide cases with similar geological characteristics, the landslide disaster prevention project will be more efficient. When designing a prevention scheme for a landslide, it is necessary to fully consider the landslide profile, which contains many landslide geological characteristics. If several landslide cases with similar geological characteristics are recommended for reference, the economic and applicable landslide treatment scheme can be formulated quickly. The geological characteristics of these landslides can be easily extracted from the landslide profile images, but the influence of these geological characteristics on the landslide treatment project should be considered comprehensively. Among them, different landslide geological characteristics have different effects on landslide disaster prevention project. In order to select suitable landslide cases for reference, this paper designs a recommendation system to recommend 5 landslide treatment cases with the similar geological characteristics for the landslide to be treated. The recommendation system fully considers the weight of different landslide geological characteristics. Finally, the results show that the landslide cases recommended by the recommendation system have high similarity with landslide.

2. Method

Our proposed approach is depicted in Fig. 1.

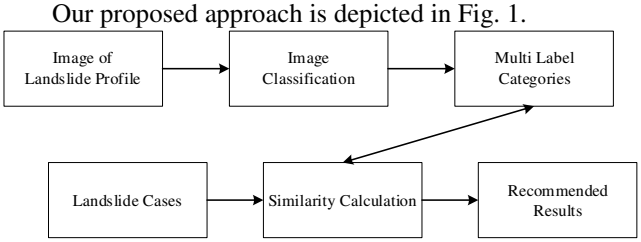


Fig.1 Flowchart of recommendation system of landslide cases

First, we clean the collected landslide profile data and make the landslide profile images needed in this study.

Then, these images are divided into training set and test set, and the classifier is trained by RF [1-3]. The classifier can be used to obtain the multi label categories of landslide geological characteristics reflected by the landslide profile image.

Finally, after obtaining the multi label categories of the landslide, we calculate the similarities among the landslide and the landslide cases, and recommend the first five similar landslide cases.

3. Data

3.1. Data source

The data in this paper was from the Sichuan Research Institute for Eco-System Restoration & Geo-disaster Prevention. The landslide profile images are mainly included in the field investigation form and the landslide disaster prevention project design survey map, which are saved as the vector image with the big scale of 1:2000, 1:800 and so on.

3.2. Landslide profile image

In ArcGIS editing state, the landslides of different scales are zoomed to the same scale. Then, different attribute values are assigned to the landslide body and sliding bed of the landslide profile as the distinction. Finally, the vector map is transformed into raster map and then converted into ASCII text. During the research process, image data will be extracted from the text and saved as an array of 32*32. The landslide profile image is shown in Fig.2, and the yellow part is the landslide body and the green part is the sliding bed.

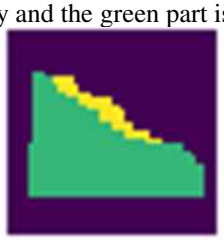


Fig. 2 Landslide profile image

4. Image classification

In this paper, in order to describe the geological characteristics of the landslide more precisely, we classify the landslide profile images by multi label. Only when the geological characteristics of the landslide are described more precisely, the good recommendation results can be obtained in the subsequent recommendation system.

4.1. Multi label categories

The multi label categories here refer to the categories of landslide geological characteristics. We describe the landslide geological characteristics by classifying the images of landslide profile.

Landslide profile image has sufficient research value and is widely used in landslide dynamic analysis, characteristic description and stability analysis [4]. In this paper, the classification of landslide profile is mainly based on 7 geological characteristics of landslide [5], as follows.

(1) **Existence of free face on the foot of slope (EF):** Generally speaking, the existence of free face on the foot of slope is caused by human excavation or rainwater scouring. It has a great impact on the stability of the landslide, and it should be considered when taking treatment measures.
(2) **Slope steepness (SS):** Generally, the steep slope is more prone to landslide than the gentle slope
(3) **Length of landslide (LL):** The length of landslide is related to the quantity and scheme of treatment measures.
(4) **Strength of sliding force (SF):** The sliding force of traction type landslide (the lower part of the landslide slides first) and the push type landslide (the upper layer slides and the lower part deforms) is stronger.
(5) **Thickness of the back edge (TB):** It used to describe the scale of landslide.
(6) **Thickness of the middle (TM):** Same as (5).
(7) **Thickness of the front (TF):** Same as (5).

4.2. Construction of landslide classification model

In this paper, we use random forest algorithm to classify landslide profile image according to the landslide geological characteristics, and then obtain the detailed categories of landslide geological characteristics. The 500 training data are divided into verification set and training set. The validation set takes 20% of the data set, and the training set takes 80% of the data set. Each landslide profile image is saved as an array of 32 * 32. In the aspect of feature extraction, we scan the rows and columns of the array, and then calculate the total number of attribute value in each row and column. Finally, we get a feature array with length of 64 as the feature representation. In order to improve the classification accuracy of the whole model, we divide the classification task into four classifiers. The parameters of

each random forest classifier are adjusted by grid search method, and the parameters of n_estimators and max_features are mainly adjusted [1]. It is found that when the values of n_estimators and max_features of the four classifiers are [(n_estimators, max_features)] = [(70, 11), (130, 5), (70, 15), (160, 15)], the whole classification model is best. Finally, the training accuracy of the whole model is 92%, and the verification accuracy is 87%. The model has good effect and meets the expectation.

5. Landslide case recommendation system

After obtaining the multi label classification results of landslides by image classification, we calculate the similarity among the landslide and landslide cases.

Euclidean distance [6] is the most common distance measure, which measures the absolute distance between points in multidimensional space. The formula is as follows:

$$\mathrm{dist}(X,Y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \quad (1)$$

where X and Y are two samples, x_i and y_i represent the eigenvalues of the ith feature of two samples respectively.

Due to the different influence degree of different landslide geological characteristics in the field of landslide treatment project, it is necessary to fully consider their respective weights. The weighted Euclidean distance is a distance measure with weight taken into account. The formula is as follows:

$$\mathrm{dist}^*(X,Y) = \sqrt{\sum_{i=1}^{n}\alpha_i(x_i - y_i)^2} \quad (2)$$

where α_i represent the weight of the ith feature, which is obtained by domain knowledge and factor analysis.

So, we use the weighted Euclidean distance as the similarity measure, in which the weight is determined by professional domain knowledge and the correlation analysis of landslide characteristic factors. The weight array is [EF, TB, TM, TF, SS, LL, SF] = [1.6, 0.6, 1.7, 0.7, 0.6, 0.3, 1.7].

6. Experiments and discussions

For the landslide profile image of a landslide, we first classified the image by classifier to obtain the multi label categories of the landslide, and then calculated the similarity among landslide cases and the landslide. Finally, five landslide cases with the highest similarity were obtained as the recommendation results. The results of recommended were shown in Fig.3, the first line of the map was the testing landslide, and the five images in the second line were recommended landslides case, and the similarity decreases from left to right. In order to evaluate the recommendation system more fully, we chose the Precision, Recall, and F-measure [7] as the evaluation. In the recommended test, we used 50 landslide cases for testing. The results were shown in Fig.4.

It could be seen from Fig.3 that the five recommended landslide cases (second line in Fig 3) are similar in these landslide geological characteristics with the testing landslide (first line in Fig.3). Please note that we only focus on the landslide body (yellow part). The sliding bed (green part) of the map is to show the landslide profile completely.

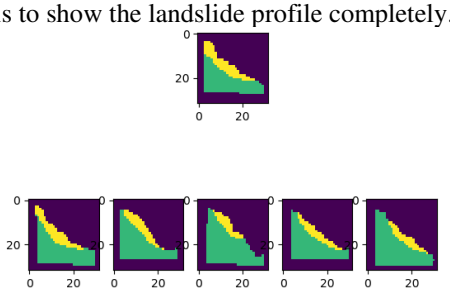
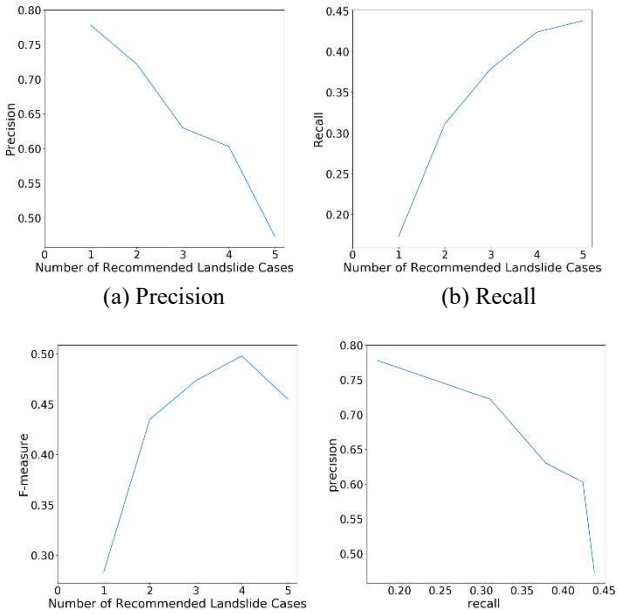


Fig.3 Recommended result



(a) Precision (b) Recall

(c) F-measure (d) PR curve

Fig.4 Precision, Recall, F-measure and PR curve

First, it can be also seen from Fig.3 that the slope of the testing landslide (first line in Fig.3) is steep, the thickness of the back edge and middle are thick, the thickness of the front is thin, the foot of slope is gentle without free face, and the length is long.

Then, we analyze the similarity between the five recommended landslide cases (second line in Fig 3) and the testing landslide (first line in Fig 3), as follows.

1) The five recommended landslide cases are relatively steep in aspect of slope steepness. It has a high similarity with the testing landslide and meets the recommended requirements.
2) The first three of the five recommended results have the characteristics of thick back edge, thick middle part, and thin front edge. Meet the recommendation requirements with high similarity.
3) Among the five recommended results, except for the third landslide case that has free face on the foot of slope, the other four recommended landslide cases and the testing landslide do not have free face.

In terms of landslide length, four of the five recommended results are close to the testing landslide, while the third recommended landslide case is not so good. Because the importance of length features is not high, so the weight of similarity calculation is low.

Finally, in general, the 5 recommended landslide cases are similar to the testing landslide to a certain extent, especially the first recommended landslide case has high similarity with the testing landslide, which has high reference value.

From the Fig.4, we can get the following observations: the precision (Fig.4 a) of the first result of recommendation exceeds 0.75. From the PR curve (d), we can know that if we refer to more recommended results for each time, we can obtain more similar landslide cases. However, the precision will be reduced at the same time. F-measure (c) considers this situation, and the value of F-measure reaches the peak when the number of recommended landslide cases is 4. This shows that, considering the precision and recall rate at the same time, the reference effect reaches the maximum when referring to the first four landslide cases.

7. Conclusion and Future Work

At present, most of the research on landslide disaster prevention project relies on expert experience, and there is little research on the combination of landslide and big data. In this paper, we used data mining and machine learning methods to describe the landslide more precisely and standard by classifying the landslide profile image. And then we build a recommendation system to provide 5 similar landslide cases, the precision of the first recommended result of each recommendation exceeds 0.75.

Acknowledgements

The work was supported in part by the Open Fund of Key Laboratory of Urban Land Resources Monitoring and Simulation, Ministry of Natural Resources (Grant No. KF-2019-04-074, Grant No. KF-2019-04-069, and Grant No. KF-2018-03-063); Open Fund of State Key Laboratory of Water Resources and Hydropower Engineering Science (Grant No. 2014SWG04, and Grant No.2018SWG02); Science Research Program of Natural Resources Department of Sichuan Province (Grant No. KJ-2020-3); and Opening Foundation of Guangxi Key Laboratory for Spatial Information and Geomatics, Guangxi, China (Grant No. 17-259-16-14 and Grant No. 19-050-11-06), The Key Technologies Research and Development Program of Sichuan Province (Grant No. 2020YFSY0041).

References

[1] Breiman L. Random Forests [J]. Machine Learning, 2001, 45(1):5-32.
[2] Ristin M, Guillaumin M, Gall J, et al. Incremental Learning of Random Forests for Large-Scale Image Classification [J]. IEEE Transactions on Pattern Analysis & Machine Intelligence, 2016, 38(3):490-503.
[3] Li B, Yang G, Wan R, et al. Comparison of random forests and other statistical methods for the prediction of lake water level: a case study of the Poyang Lake in China[J]. Hydrology Research, 2016, 47(S1):69-83.
[4] Li L, Lan H, Strom A. Automatic generation of landslide profile for complementing landslide inventory [J]. Geomatics, Natural Hazards and Risk, 2020, 11(1):1000-1030.
[5] Guofu S, Weining L, Lianjin T, et al. Failure mechanism and modeling of excavation effect for steep over-dip stratified rock slope [J]. Chinese Jounal of Geotechnical Engineering, 2003.
[6] Runtao T, Peishan X. Study on the Standardization of Similarity Evaluation Method of Chromatographic Fingerprints (PartI) [J]. Traditional Chinese Drug Research & Clinical Pharmacology, 2006.
[7] Huang W, Kataria S, Caragea C, et al. Recommending citations: Translating papers into references[C]// 21st ACM International Conference on Information and Knowledge Management, CIKM'12, Maui, HI, USA, October 29 - November 02, 2012. ACM, 2012.

CLASSIFICATION OF LANDSLIDE STABILITY BASED ON FINE TOPOGRAPHIC FEATURES

CHAO WANG[1], MING-CANG ZHU[2], ZHI-GANG MA[3], ZHAN-YONG HE[3], HONG JIANG[3], PENG-SHAN LI[4], XIAO-BO ZHANG[5], JI-BAO SHI[5], KAI CHEN[5], TAO WENG[5], ZE-ZHONG ZHENG[1]*, QIANG LIU[1]*, FANG HUANG[1]

[1]School of Resources and Environment, University of Electronic Science and Technology of China, Chengdu, Sichuan, PRC 611731
[2]Department of Natural Resources of Sichuan Province, Chengdu, Sichuan, PRC 610072
[3]Sichuan Research Institute for Eco-System Restoration & Geo-disaster Prevention, Chengdu, Sichuan, PRC 610081
[4]Chengdu Land Planning and Cadastre Center, Chengdu, Sichuan, PRC 610074
[5]Chengdu Institute of Survey & Investigation, Chengdu, Sichuan, PRC 610081
E-MAIL: zezhongzheng@uestc.edu.cn.

Abstract:

In this paper, we propose an extraction method for landslide topographic features and based on these fine features, we trained a landslide stability classification model. Topographic factors have a huge impact on the stability of landslides, and our new feature extraction methods can provide more accurate portraits of landslides. Considering the factors affected landslide stability, this paper studied the factors used in traditional quantitative stability calculations and analyzed the factors affecting stability based on landslide data. So, the proposed method is a combination of theoretical method and numerical method. Based on support vector classification (SVC), random forest (RF), and extreme gradient boosting (XGBoost) models, this paper compares and analyzes the rationality and reliability of the landslide stability classification results output by three models. After adopting the new fine feature extraction method, the accuracy of the stable classification results has been improved by about 5% on average, and the interpretability of the classification results has also been greatly enhanced.

Keywords:

Landslide stability classification; Feature extraction; Topography feature; Machine learning.

1. Introduction

Landslides are common natural disasters that often cause serious impact and damage to human society. Landslide stability evaluation is crucial. Landslide stability evaluation methods are mainly divided into qualitative and quantitative methods. The qualitative method is highly subjective, and sometimes it just relies on expert judgment. The quantitative method, the method based on statistical learning is currently popular, and there are many successful cases [1]. This method uses machine learning or statistical models to modeling and analysis of landslide data.

Up-to-date studies on landslides stability, many studies use the topography data in the landslide disaster field survey to study the stability of landslides through machine learning methods. The landslide disaster field survey has topographic data as average slope, main aspect, curvature and elevation range. But topography data in the landslide disaster field survey is not enough fine to reflect the characteristics of the landslide [2]. This paper used 129 samples of landslide treatment projects to analyze and extract their fine topographic features. Then we built multiple landslide stability classification models based on original topographic feature and fine topography features and selected the optimal models from a number of models.

2. Method

Our proposed approach is depicted in Fig. 1.

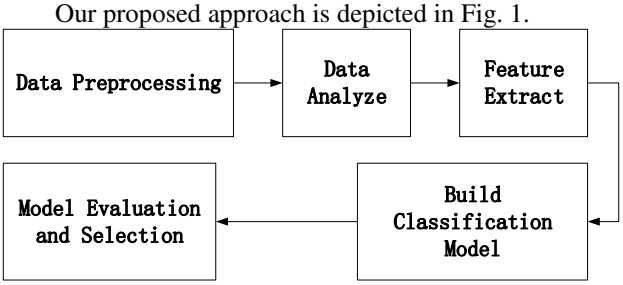


Fig.1 Flowchart of classification of landslide stability

First, we collected landslide topographic data from the landslide treatment engineering data. We preprocessed the landslide topographic data, and converted the topographic

data of the landslide area into TXT format. In order to facilitate further analysis, we converted the landslide topographic data into a two-dimensional matrix.

Then, in order to ensure that the selected topographic factors can well reflect the stability of the landslide, this paper used the chi-square test to evaluate the correlation between topographic factors and landslide stability.

Next, we used selected topographic factors with the highest chi-square test scores for feature extraction. We carried out feature extraction based on some engineering experience of landslide treatment, this may also be beneficial to explain why our models perform better than others. We used the original topographic features and fine topographic features for comparison.

Finally, we trained various classification models such as SVC, RF, XGBoost. And we got good results through these models.

3. Feature Engineering

3.1. Data Preprocessing

This paper extracted data such as elevation points and landslide range from the preliminary design drawings of the landslide treatment project. Using the tools in the ArcToolbox, the elevation point data is used to generate the DEM （Digital Elevation Model) of the landslide area. Then, based on the landslide range, we can accurately cut out 129 landslide DEMs. Based on the DEM data of landslide, we used the tools in Arctoolbox to get the slope data, aspect data, curvature data. Finally, we exported the raster data of each landslide into TXT format and read it automatically by the python program.

After the previous data processing, we obtained 129 landslide samples, and each landslide sample has data on elevation, slope, aspect, curvature and shape. The data of elevation, slope, aspect, curvature and shape are all two-dimensional matrices. In order to facilitate the subsequent analysis, each matrix was transformed into 64×64 matrix.

3.2. Data Analyze

In previous landslide stability studies, the slope, aspect, elevation, and curvature were considered when considering topographic features.

In this paper, we used the chi-square test method [3] to evaluate the correlation between the selected topographic factors and the stability of the landslide.

Here we choose χ^2 score:

$$\chi^2 = \sum \frac{(A-E)^2}{E} = \sum_{i=1}^{k} \left(\frac{A_i - E_i}{E_i}\right)^2 = \sum_{i=1}^{k} \left(\frac{A_i - p_i}{np_i}\right)^2 \quad (1)$$

Among them, Ai is the horizontal observation frequency of i, Ei is the expected horizontal frequency of i, n is the total frequency, pI is the expected frequency for the level of i. The calculated result is used as the score of the chi-square test. The higher the score, the higher the importance of the feature.

Table 1 χ^2 test score of factors

Factors	χ^2 test score
Slope	20.18
Elevation	14.70
Curvature	11.42
Aspect	6.46

In the chi-square test results of all topographic factors, slope, elevation, and curvature have greater influence on the stability of the landslide than the aspect.

3.3. Feature Extract

In some previous machine learning studies on landslides, for topographic features, only the average slope, main slope direction, curvature, and elevation interval of the landslide were roughly extracted. This paper refines the topographic features of landslides, and proposes a more refined way of extracting topographic features of landslides based on landslide stability theory and treatment experience.

Thanks to the precious field survey data, we can extract the topographic features of each part of each landslide.

For elevation data, its influential features include average elevation, maximum elevation, minimum elevation, and variance of elevation. The relative elevation and height difference can better reflect the stability of the landslide.

For slope data, we are not only concerned about its maximum and minimum values, we are more concerned about the trend of slope changes along the landslide. The slope distribution has a huge impact on the stability of the landslide. For example, when the slope of the front edge of a landslide is relatively large, an empty surface will be produced, which is very detrimental to the stability of the landslide.

For aspect data, statistical analysis is performed to get histogram features. The aspect value is distributed between 0 to 360. The range of aspect is divided into multiple sections with an interval of 45 degrees: [22.5, 67.5, 112.5, 157.5, 202.5, 247.5, 292.5, 337.5]. These eight sections represent the eight directions of north, northeast, east, southeast, south, southwest, west, and northwest.

For curvature data, we extract the absolute value of the curvature and the positive and negative distribution. The plus or minus of the curvature value can determine whether a

certain part of the surface is convex or concave. This is related to groundwater and surface runoff.

4. Model of classification

We try to use SVC, RF, and XGBoost methods to evaluate the stability of landslide. We divide the landslide data into two parts, a training set and a test set. We randomly split the training set and test set according to the ratio of 8:2. Each landslide has its stability label. Then, we begin to build classification model through machine learning methods.

SVC is a classification algorithm. It is a classification model. Its basic model is defined as the linear classifier with the largest interval in the feature space, that is, the learning strategy of the support vector machine is to maximize the interval, which can finally be transformed into the solution of a convex quadratic programming problem.

RF is a member of the ensemble learning family, and it's a bagging method. Random forest is a combination of a series of decision trees, and the samples when each tree is constructed are sampled from the training set after replacement [4].

GBDT is also a member of the ensemble learning family, and its weak learner can be Classify and Regression Tree (CART) [5]. The XGBoost classification algorithm is evolved from the GBDT algorithm. The base classifier of the algorithm is a decision tree, which improves the classification effect of the model while continuously increasing the number of decision trees in the classifier.

We use the original features extracted from the landslide field survey form and the fine features extracted through the refined landslide feature extraction method to train the landslide stability classification model. We build the classification of landslide stability with SVC, RF, and XGBoost models. In the classification model, to evaluate the effect of the model, the commonly used evaluation indicators include accuracy and recall. We also use test set data to evaluate the classification models. The results were shown in Table 2.

Table 2 Accuracy and Recall of models

Method	Accuracy	Recall
SVC (original feature)	0.71	0.85
RF (original feature)	0.82	0.89
XGBoost (original feature)	0.85	0.92
SVC (fine feature)	0.76	0.86
RF (fine feature)	0.88	0.91
XGBoost (fine feature)	0.89	0.94

5. Experiments and discussions

It could be seen from Table 2 that for SVC model has the lowest accuracy and recall rate. Ensemble learning methods have better performance than single machine learning methods. We use accurate and fine landslide measurement data to extract influential feature. Based on fine topographic features, we get better landslide stability classification model. The accuracy of the classification model with fine topographic features is 0.04 to 0.05 higher than the classification model trained with the original topographic features. The RF and XGBoost models perform well in classification accuracy and recall rate. XGBoost has an accuracy rate of 0.89 and the highest recall rate, reaching 0.94. From the result of classification, the performance of XGBoost and RF are apparently better than SVC, mainly because they are all ensemble models, which have a good suppression of noise in data.

The results of stability classification are consistent with the results of quantitative analysis of landslide stability, indicating that the classification results have high reliability and the model has good application value.

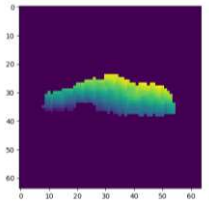


Fig. 1 Elevation

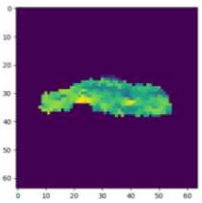


Fig. 2 Slope

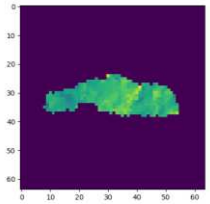


Fig.3 Aspect

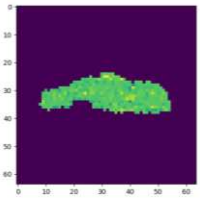


Fig.4 Curvature

From Fig.1 to Fig.4, we can see that the topographic of landslide of Peach Garden, Santai County. The color shade in the picture represents the value, and the value decreases from yellow to green to blue. According to the stability classification model, this landslide is relatively stable. We can see that the lateral distance of this landslide is much longer than its longitudinal distance, the middle part is steeper and the front and rear edges are gentler. The curvature changes smoothly and there is no mutation site. Its front edge does not have an empty surface where landslide is easy to slide out. So, landslide of Peach Garden, Santai County is in good stability. The classification results are

consistent with the conclusions drawn from the theoretical and practical experience of the landslide survey.

6. Conclusion and Future Work

At present, when using machine learning to study landslide stability, the extraction of topographic features is very rough. Existing research simply regards the landslide, and uses the average slope, main slope direction, curvature and elevation interval as the topographic features of the landslide for machine learning classification. In this paper, a new feature extraction method is used to better reflect the topographical features of the landslide. In addition to considering the overall characteristics of the landslide, the features of each part of the landslide are also extracted. The new features can better represent the topographic of the landslide, which is more beneficial to the study of landslide stability. By adopting new and more refined features, the accuracy and recall rate of the landslide stability classification model have been improved.

Acknowledgements

The work was supported in part by the Open Fund of Key Laboratory of Urban Land Resources Monitoring and Simulation, Ministry of Natural Resources (Grant No. KF-2019-04-074, Grant No. KF-2019-04-069, and Grant No. KF-2018-03-063); Open Fund of State Key Laboratory of Water Resources and Hydropower Engineering Science (Grant No. 2014SWG04, and Grant No.2018SWG02); Science Research Program of Natural Resources Department of Sichuan Province (Grant No. KJ-2020-3); and Opening Foundation of Guangxi Key Laboratory for Spatial Information and Geomatics, Guangxi, China (Grant No. 17-259-16-14 and Grant No. 19-050-11-06), The Key Technologies Research and Development Program of Sichuan Province (Grant No. 2020YFSY0041).

References

[1] Zhuang Yulong, Tian Yuan, and Cheng Chuyun. "Evaluation of Landslide Risk Based on Deep Neural Network –Take Shenzhen as an example." Geography and Geo-Information Science (2019):2-26. vol. 34, No 2, p104.

[2] Han, Z., Su, B., Li, Y. et al. " Comprehensive analysis of landslide stability and related countermeasures: a case study of the Lanmuxi landslide in China. " Sci Rep 9, 12407 (2019).

[3] Donald Sharpe. "Your Chi-Square Test Is Statistically Significant: Now What? " Practical Assessment, Research & Evaluation Volume 20, Issue 8, 2015, PP 1-10

[4] F. VERONESI, L. HURNI. Random Forest with semantic tie points for classifying landforms and creating rigorous shaded relief representations[J]. Geomorphology. 2014, 224(1): 152- 160

[5] Friedman, Jerome H. "Greedy Function Approximation: A Gradient Boosting Machine." The Annals of Statistics 29.5(2001):1189-1232.

A NON-PARAMETRIC MULTI-LINGUAL CLUSTERING MODEL FOR TEMPORAL SHORT TEXT

JAY KUMAR[1], RAJESH KUMAR[1], AMIN UL HAQ[1], SIDRA SHAFIQ[2]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China
[2]Department of Computer Science, The Women University Multan, Punjab, Pakistan
E-MAIL: jay@std.uestc.edu.cn, rajakumarlohano@gmail.com

Abstract:

Short text data is being continuously generated by many social streams such as Facebook and Twitter. Clustering the temporal text, data for the sake of identifying new topics, over huge volume of data has become very challenging task recently. Apart from supervised approaches, most of the existing clustering approaches assume that the input data belong to one language. Whereas, generally it has been observed that multi-lingual short text on social media exist in bulk amount. In this paper, we propose a model to cluster unknown number of topics in temporal environment for multi-lingual data. The proposed framework integrates non-parametric dirichlet model with language translation component (NDML) to cluster the temporal stream of short text data, and transforms the cluster feature into uniform language vector representation. We conducted experiments on real time crisis data to evaluate the accuracy of our proposed model.

Keywords:

Dirichlet model; Temporal data; Stream clustering; Multi-lingual Text

1. Introduction

During the past decade, social media and digital news platforms have become vital source of information for many global events or emergencies. A huge volume of text data is generated everyday containing critical events over time. The task of clustering such stream of text data has attracted attention of researchers in recent years. However, due to temporal dependencies of text data and unknown number of events make this task very challenging. Along with these constraints, generally a massive amount of generated text data belongs global events such as disaster, crisis and safety warnings thus contain multi-lingual information [1].

A series of models to deal with multi-lingual data has been proposed in the literature. Each model has its own benefits and disadvantage. [2] proposed a cross-lingual tweet classification M-BERT model with employing mixup manifold. However, it is necessary to pre-define the number of classes to train M-BERT for downstream task. In addition, class specific features highly rely while training phase. Usually previous models used original terms to fed the classification model, but [3] explored exploited semantic and statistical features to improve the classification accuracy on multi-lingual text data. Previous research on event discovery from news using evolution graph has been introduced [4], but it is not fit for short text [12]. Additionally, it needs a pre-defined number of classes to train the model. Most approaches are supervised and do not consider temporal dependency [5]. Where, [6] and [7] proposed short text clustering model, however their approach deal with monolingual text data. Therefore, there exist need a general framework to overcome mentioned issues together.

In this paper, we propose a framework which builds a bridge between clustering model and language translation component. We employ non-parametric dirichlet clustering model (NDML) to cluster the temporal short text data and build a bridge to identify the events based on change in probability distribution. The temporal data is splitted into fixed window, then dirichlet model update the existing model either by merging each instance into existing cluster or create a new cluster. The continuous updated model having active clusters is then processed to label the cluster related to different language using translation component. Furthermore, we exploit the word hypernym to expand the cluster features for performance improvement. The main contributions of our work are defined as follows.

- We propose a model to cluster multi-lingual temporal text data.
- Proposed approach can identify evolving number of events from generated text from social streams.
- We conducted empirical study to evaluate and prove the significance of our model.

2. Proposed Model

To solve the problem of identifying continuous arrival of events from temporal text data, we propose a framework (NPML), a non-parametric dirichlet model based clustering for multi-lingual data. Figure 1 shows our proposed architecture. In the initial step, streaming1 data is sliced into chunks. These chunks are either based on time-window or fix-sized window. The former type of chunk consider instances in time unit i.e., hour, day, or week. The latter type of chunk consider static number of instances for each window. Then, each chunk is fed into dirichlet model to group the short text instances. Within the existing model, each instance of chunk either merged into existing cluster or create a new cluster. Afterwards, each cluster' features are passed into translation process where clusters having same topics (based on similarity discussed in Section III) with different language are assigned with common label. We define each component in detail.

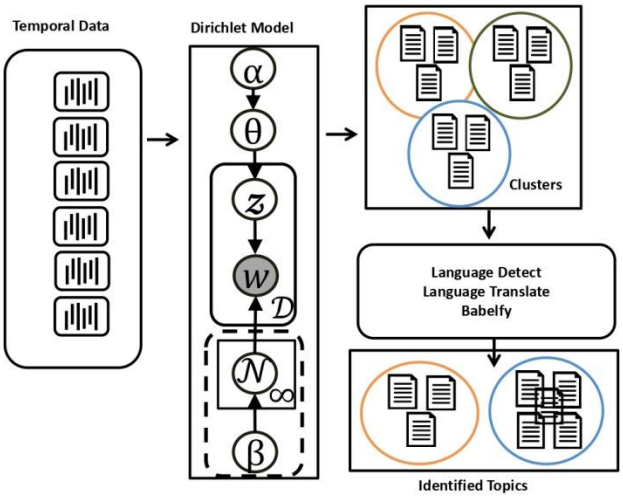


Fig.1 The proposed model for multi-lingual text clustering.

2.1. Non-parametric Dirichlet Model (NDM)

It is a type of stochastic model which models the random procedure of generated objects from a pre-defined distribution. A variety of dirichlet models have been proposed in the past, however, recently, [7] proposed a model based on Chinese Restaurant Process (CRP) to deal with temporal data to capture infinite number of topics. We exploit this model to cluster the incoming documents from temporal stream. This model is specifically designed for short text stream clustering task. The model specifies the probability to calculate incoming document and existing cluster, defined in Equation (1).

$$p\left(z_d = z \mid \vec{d}\right) = \left(\frac{n_z}{D-1+\alpha D}\right) \cdot \left(\frac{\prod_{w\in d}\prod_{j=1}^{N_d^w}\left(v_z^w\right)+\beta+j-1}{\prod_{i=1}^{N_d^z} l_z+(V\beta)+i-1}\right) \quad (1)$$

To create a new cluster, the defined probability is give n in Equation (2).

$$p\left(z_d = z_{new} \mid \vec{d}\right) = \left(\frac{\alpha D}{D-1+\alpha D}\right) \cdot \left(\frac{\prod_{w\in d}\prod_{j=1}^{N_d^w}\beta+j-1}{\prod_{i=1}^{N_d}(V\beta)+i-1}\right) \quad (2)$$

Here, n_z represents total number of documents in the cluster, N_d^w total unique terms in the document, D rep resents the current number of clusters in the model, V specifies the total vocabulary of current cluster, N_d is the length of document in terms of words, and v_z^w re present frequency count of term w in cluster z. The n otation α and β are model parameters. The incoming d ocument can create new cluster if probability in Equati on (1) is greater than Equation (2) for all existing clus ters.

2.2. Cluster Feature Set

The vector space model (VSM) is generally used for clustering task. However, to represent a cluster into subspace, we employ cluster feature set (CF) [8]. A CF is defined as Each cluster is represented by words of related documents. In our model, we followed [7] and define CF set as a 3-tuple $\left\{n_z, v_z^w, l_z\right\}$. Here, n_z represents number of documents in the cluster, d_z^w represents frequency of each unique term in cluster and l_z is total words in cluster.

2.3. Language Translation Component

We build a translation component by cascading detectlanguag[1], google-translate[2] and Babelfy[3]. The first library detects the language to transfer the input for translation into English language. Afterwards, Babelfy library is used to fetch hypernyms of key terms of cluster features. The extracted hypernyms of terms help to calculate

[1] https://detectlanguage.com
[2] https://translate.google.com
[3] https://babelfy.org

similarity between two different clusters of different language [9]. The reason to identify the language is to avoid calculating distance between clusters of same topics. We calculate both probabilities in Equation [1] and Equation [2] to calculate similarity to relate two clusters of same topics. Here, instead of using model vocabulary, V represent the cluster local vocabulary.

3. Experiments

This section discusses the experimental setup of evaluate our model. We define the process of constructing dataset. We also describe selected state-of-the-art algorithms to compare the performance with detail discussion. As we already mentioned that we employ NDM for clustering the short text, which relies on two parameters. Therefore, we also demonstrate the effect of these parameters in terms of three different evaluation measures.

3.1. Data set

For our empirical study, we downloaded SOSItalyT4[4], ChileEarthquakeT1, and CrisisLexT26 from the CrisisLex platform to construct a dataset. It contains 26 crisis or disaster events occurred during 2009 to 2014 around the world, hence documents are related to different languages. Along with removing the special characters, we deducted all duplicate instances from the individual datasets to reduce content redundancy. Table 1 shows the statistics of constructed dataset.

Table 1 Dataset Statistics

Language	Documents	Vocabulary	Topics
English	5171	18140	26
Italian	3239	11301	26
Spanish	3788	12133	26
Total	12198	41574	26

3.2. Models for Comparison

To compare with our model, we choose two supervised deep neural network model, M-BERT and FastText [10]. M-BERT is multi-lingual pre-trained BERT [11] model on multi-lingual data from wikipedia. We set $batchsize = 32$, a learning rate between 10-3 and a fine-tuning rate of 2×10^{-5}. We run each selected model five times and then calculate the average performance. As we already mentioned, these models are fully supervised, therefore we employ 3-fold cross validation to evaluate the models. Although, our proposed model follows fully unsupervised setting.

3.3. Results Discussion

We trained the chosen models on two types of feature sets. The VSM representation on actual terms of text, referred as "ofs" and extended feature set using hypernyms of key terms referred as "hyper". As the results of all the models can be seen in Table 2. In terms of accuracy and recall, our model outperformed the BiLSTM and FastText. The reason behind is the limited training dataset to learn the network weight in multi-lingual instance. Whereas, M-BERT is specifically pre-trained to multi-lingual data that is the reason it performed well with limited training instances. It can be clearly observed that using hypernym as additional information improves the model performance.

Model	ofs	hyper	ofs	hyper
	Accuracy		Recall	
M-BERT	81.39	83.49	83.59	84.33
FastText	73.79	74.90	74.83	75.55
BiLSTM	72.40	73.10	73.44	74.20
NDML	79.22	83.51	80.32	84.48

3.4. Parameter Sensitivity

We analyzed the two hyper-parameters of NDM for further investigation of clustering quality. The Figure 2 and Figure 3 show the sensitivity of α and β, respectively, with respect to Normalized mutual information (NMI), accuracy, and homogeneity (Ho). From the the given plots we can clearly observe that the model in the streaming environment does not show a high variance over a significant range of values.

4. Conclusion

In this paper, we propose short text clustering framework by integrating non-parametric dirichlet model (to cluster short text) with language translation module to identify event in multi-lingual social stream. In contrast to existing approaches, NDML do not require pre-defined number of events and cluster continuous arrival of text instances in temporal dependency scenario. More importantly, we tried to explore the hypernym using Babelfy to expand the core terms of each cluster. The given empirical results demonstrate the significance of our model.

[4] https://crisislex.org

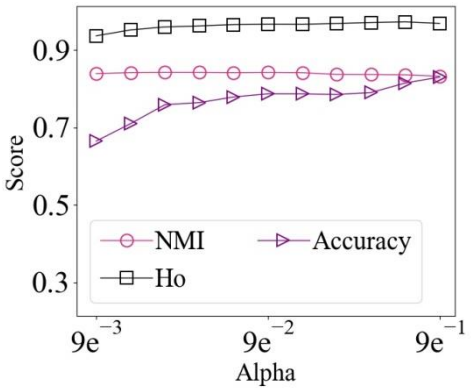


Fig.2 The sensitivity of α parameter.

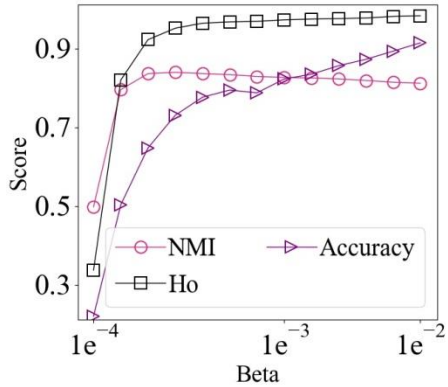


Fig.3 The sensitivity of β parameter.

References

[1] N. D. Doulamis, A. D. Doulamis, P. C. Kokkinos, and E. M. Varvari- gos, "Event detection in twitter microblogging," IEEE Trans. Cybern., vol. 46, no. 12, pp. 2810–2824, 2016.

[2] J. R. Chowdhury, C. Caragea, and D. Caragea, "Cross-lingual disaster- related multi-label tweet classification with manifold mixup," in Pro- ceedings of the 58th Annual Meeting of the Association for Computa- tional Linguistics: Student Research Workshop, ACL 2020, Online, July 5-10, 2020. Association for Computational Linguistics, 2020, pp. 292–298.

[3] P. Khare, G. Burel, D. Maynard, and H. Alani, "Cross-lingual clas- sification of crisis data," in The Semantic Web - ISWC 2018 - 17th International Semantic Web Conference, Monterey, CA, USA, October 8-12, 2018, Proceedings, Part I, vol. 11136. Springer, 2018, pp. 617–633.

[4] Y. Liu, H. Peng, J. Li, Y. Song, and X. Li, "Event detection and evolution in multi-lingual social streams," Frontiers Comput. Sci., vol. 14, no. 5, p. 145612, 2020.

[5] K. K, Z. Wang, S. Mayhew, and D. Roth, "Cross-lingual ability of multilingual BERT: an empirical study," in 8th International Conference on Learning Representations, ICLR 2020, Addis Ababa, Ethiopia, April 26-30, 2020. OpenReview.net, 2020.

[6] J. Chen, Z. Gong, and W. Liu, "A nonparametric model for online topic discovery with word embeddings," Information Sciences, vol. 504, pp. 32–47, 2019.

[7] J. Yin, D. Chao, Z. Liu, W. Zhang, X. Yu, and J. Wang, "Model-based Clustering of Short Text Streams," in ACM International Conference on Knowledge Discovery and Data Mining, 2018, pp. 2634–2642.

[8] S. U. Din and J. Shao, "Exploiting evolving micro-clusters for data stream classification with emerging class detection," Information Sci- ences, vol. 507, pp. 404–420, 2020.

[9] H. Gong, T. Sakakini, S. Bhat, and J. Xiong, "Document similarity for texts of varying lengths via hidden topics," in Proceedings of the 56th Annual Meeting of the Association for Computational Linguistics, vol. 1, 2018, pp. 2341–2351.

[10] Joulin, E. Grave, P. Bojanowski, M. Douze, H. Je´gou, and T. Mikolov, "Fasttext.zip: Compressing text classification models,"CoRR, 2016. [Online]. Available: http://arxiv.org/abs/1612.03651

[11] J. Devlin, M. Chang, K. Lee, and K. Toutanova, "BERT: pre-training of deep bidirectional transformers for language understanding," in Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, 2019, pp. 4171–4186.

[12] Z. Saeed, R. A. Abbasi, A. Sadaf, M. I. Razzak, and G. Xu, "Text stream to temporal network - A dynamic heartbeat graph to detect emerging events on twitter," 2018, doi: 10.1007/978-3-319-93037-4_42.

RECOGNIZING EMOTIONS FROM TEXTS USING A BERT-BASED APPROACH

ACHEAMPONG FRANCISCA ADOMA[1], NUNOO-MENSAH HENRY[2], WENYU CHEN[1], NIYONGABO RUBUNGO ANDRE[1]

[1]Computational Intelligence Lab, School of Computer Science and Technology, University of Electronic Science and Technology of China, Chengdu, China
[2]Connected Devices Lab, Department of Computer Engineering, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana
E-MAIL: francaadoma@gmail.com, hnunoo-mensah@knust.edu.gh, cwy@uestc.edu.cn, niyongabor.andre@gmail.com

Abstract:

The popularity of using pre-trained models results from the training ease and superior accuracy achieved in relatively shorter periods. The paper analyses the efficacy of utilizing transformer encoders on the ISEAR dataset for detecting emotions (i.e., anger, disgust, sadness, fear, joy, shame, and guilt). This work proposes a two-stage architecture. The first stage has the Bidirectional Encoder Representations from Transformers (BERT) model, which outputs into the second stage consisting of a Bi-LSTM classifier for predicting their emotion classes accordingly. The results, outperforming that of the state-of-the-art, with a higher weighted average F1 score of 0.73, become the new state-of-the-art in detecting emotions on the ISEAR dataset.

Keywords:

Natural language processing; Transfer learning; Emotion detection; BERT

1. Introduction

The use of computational approaches is heavily gaining traction for the detection of emotions from human-written texts. It can be attributed to the fact that challenges of word ambiguity and insufficient linguistic resources in the keyword approach have since been tackled by the emergence of various publicly available datasets and computational methods emanating from numerous natural language processing (NLP) competitions. The different available datasets are ridden with unique characteristics that make them exciting to use and quite challenging to handle. Notable among the datasets inciting text-based emotion detection activities is the ISEAR dataset [1]. The ISEAR also has its peculiar characteristic, i.e., a limited number of data samples, same sentence mapping to different emotion class labels. These make it exciting and challenging to work on the ISEAR dataset. Notwithstanding, the dataset has been explored using various statistical and deep learning models to provide competitive results in detecting emotions from texts [2]–[7]. However, most of these proposed models, the context of emotion-conveying words, were often overlooked or subtly considered [8]. Transfer learning for computational intelligence activities is gathering momentum due to the enormous advantages, viz., improved performance using fewer data samples, and shorter training time. The limited number of data samples in the ISEAR dataset makes it an appropriate candidate to utilize transfer learning.

The popularity of transformers [9] for language understanding is tremendous due to the enhanced performance they achieve in everyday text-based emotion detection tasks and other NLP tasks [10]–[12]. The encoder and self-attention layers implemented in transformers aid in the extraction of intrinsic details from texts. Notably, the Bi-directional Encoder Representations for Transformers (BERT) [13] model is a pre-trained encoder-transformer model that produces useful context representations and providing state-of-the-art results in various NLP tasks [14].

The contribution of this paper is thus;

- To analyze the efficacy of utilizing encoders and transformers on the ISEAR dataset for detecting emotions (i.e., anger, disgust, sadness, fear, joy, shame, and guilt).
- To propose a two-stage architecture for detecting fine-grained emotions from sentences in the ISEAR dataset.
- To demonstrate the performance of BERT by fine-tuning on the ISEAR dataset.

The paper's organization is as follows; section 2 discusses related works; section 3 highlights the emotion detection pipeline and the model architecture. The experimental setup of the study, the dataset used, and how the model was evaluated are presented in section 4. The

results obtained and their corresponding analyses are presented in section 5. In section 6, the conclusion and future works are highlighted.

2. Related Works

Mozafari and Tahayori [5] presented a Similarity Technique based on Vector Similarity Measure (VSM) [15] and STASIS [16] method. Their work initially implemented Stasis for extracting semantic relationships from texts and then determined the similarity measure of texts using the VSM method. Their STASIS approach, however, did not leverage the co-occurrence ability of words in a sentence; thus, ignoring contextual semantics. After evaluating the ISEAR dataset [1], they found that the VSM method outperformed the Stasis and Keyword method to detect emotions into joy, sadness, anger, fear, shame, disgust, and guilt categories. Their approach attained an F1-score of 0.53.

The two-staged text feature extraction model proposed by Singh *et al*. [17] aimed at extracting semantics based on statistical scores. After applying a Parts of Speech (PoS) tagger to select the nouns, verbs, adverbs, and adjectives in a sentence, the chi-square [18] was used to remove features considered to be semantically weak. The model was evaluated using the ISEAR dataset and the Support Vector Machines (SVM) classifier and obtained an accuracy of 72.43%. The model, however, reportedly did not take into account the relationship between features.

Alotaibi [7] overcame some of the issues identified in work by Mozafari and Tahayori [5] and Singh *et al*. [17] by proposing a supervised logistic regression approach to detect emotions from texts. The data they obtained from ISEAR was divided for training and testing. In the training process, sentences carrying emotions were fed into their logistic regression model and their emotion labels. Only the unseen emotion labeled sentences were passed through the trained classifier for prediction in their testing process. They evaluated the performance of their model using the precision, recall, and F1 score. They reported an F1-score of 0.76, 0.64, 0.73, 0.62, and 0.57 for joy, fear, sadness, shame, and guilt emotion classes. They hinted that a deep learning model could perform better on engineering the features for classification.

The work by Seal *et al*. [19] searched for emotion words from a pre-trained emotional keyword database with a focus on extracting phrasal verbs that convey semantic and contextual meanings in sentences. Using the ISEAR dataset, they created a list of phrasal verbs and constructed a database for the phrasal verbs and their synonyms. Using the WordNet emotion lexicon, the power thesaurus, and their built phrasal verb database, they identified keywords and phrasal verbs associated with specific emotions and classified them accordingly. They obtained a percentage F1 score of 66.18%. Still, they highlighted that their method did not resolve problems presented in existing systems, such as the preliminary list of emotional keywords and disregard for word semantics based on context.

3. Proposed Model

3.1. Model Overview

An overview of this work shown in Figure 1 involves pre-processing data acquired from the ISEAR dataset and fine-tuning the data using the BERT pre-trained model. Extracted vector transformations are then fed into a classifier to classify sentences into seven fine-grained emotions, i.e., anger, disgust, fear, guilt, joy, sadness, and shame.

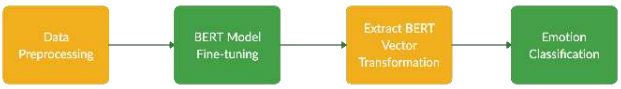


Fig.1 Overview of our proposed text-based emotion detection process

3.2. Detailed Architecture

The detailed architecture proposed is made up of two stages: BERT fine-tuned training stage and the Bi-LSTM classification stage, as shown in Figure 2.

The BERT fine-tuning stage assumes a bidirectional pre-training approach to modeling language using self-attention and transformers. This approach enables BERT to learn the context of a word considering other words in its environment.

In this work, BERT is adopted as a substructure due to this capability. Specifically, the BERT-base-uncased made up of 12-layered transformer blocks with each block containing 12-head self-attention layers and 768 hidden layers and producing approximately 110 million parameters in total, is used. The input sentences are split into tokens and mapped to their indexes in the BERT tokenizer library, indicated as input ids. It is worth mentioning that the [CLS] (classification token) and [SEP] (separate segment token) are unique tokens appended at the beginning and end of every sentence, respectively. To handle the limitations of varying lengths, an input attention mask of fixed length with 1, indicating tokens that were not padded and 0 showing padded tokens, was applied. Each of the transformers was showed a list of token embeddings and produced a feature vector of the same length at the output. The output of [CLS] for the 12*th* transformer layer containing vector transformations of prediction probabilities are used as

aggregated sequence representation from which classification is made. In the Bi-LSTM classifier stage, a Bi-LSTM with four layers, i.e., the Input layer, the Mask layer, the Bidirectional LSTM layer, and the dense layer, were attached to the BERT model. The input layer received the output of the [CLS]. The bidirectional layer consisted of 100 neurons or units and a dense layer containing seven neurons or units to predict the seven emotion classes using the softmax activation function.

4. Experiments

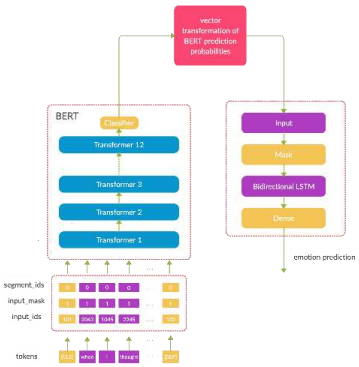


Fig.2 Proposed model showing the BERT and the Bi-LSTM-based classifier

The dataset used, how experiments were carried out, and the metrics used to evaluate the model is presented in this section.

4.1. Dataset and Setup

The ISEAR dataset comprises 7666 sentences, out of which 7503 are unique. There are seven emotion classes in the ISEAR dataset: joy, anger, sadness, shame, guilt, surprise, and fear. The data set distribution in the dataset, as seen in Table 1. The table shows that the data set does not suffer from class imbalances. It indicates that there would be no need to implement strategies to mitigate class imbalances in this data since it's already balanced. All the data samples in the dataset were used.

Table 1 Characteristics of the ISEAR Dataset

Emotion Labels	Quantity
Anger	1096
Disgust	1096
Sadness	1096
Shame	1096
Fear	1095
Joy	1094
Guilt	1093
Total	7666

Table 2 Evaluation of the ISEAR Dataset on the Model.

Classes	Precision	Recall	F1-Score
Anger	0.56	0.74	0.64
Disgust	0.83	0.62	0.71
Fear	0.89	0.84	0.86
Guilt	0.54	0.60	0.57
Joy	0.89	0.94	0.92
Sadness	0.85	0.73	0.78
Shame	0.64	0.64	0.64
Macro Average	0.74	0.73	0.73
Weighted Average	0.74	0.73	0.73

The data samples were cleaned to remove tags, double spacing, and some special characters observed to affect the detection's performance. The seven emotion classes were encoded to a numerical scale (i.e., 0, 1, 2, 3, 4, 5, 6) before the samples were split into two groups, i.e., 80% for training, 20% for testing. It was realized that the longest sentence in the dataset had 178 words; this helped in setting a maximum sentence length of 200 for the tokenizer. It was done to ensure that no sentence is truncated as BERT requires all supplied sentences to have the same size. The training and test samples were tokenized using the BERT tokenizer to generate the tokens. These tokens were encoded to create the input IDs, input mask, and segment id for each sentence denoted as ***input_ids***, ***input_mask***, and ***segment_ids,*** respectively. These were then fed to the tuned BERT model as features for training and evaluation. The training set (i.e., *trainFeatures*) was provided to the adjusted BERT model's input. The batch size, learning rate, warm up, and the number of epochs was set to 16, $2*10^{-5}$, 0.1, and 1. A total of 383 steps was used for the training per epoch. The evaluation of the model was carried out using the testing set (i.e., *valFeatures*). The model was optimized using the rectified Adam, and the loss parameter was set to *sparse_categorical_crossentropy*. The model was trained for ten epochs before being tested on the testing set.

4.2. Evaluation Metrics

To ensure the constructive and extensive comparison of the proposed model with existing models, the accuracy, precision, recall, and F1-score evaluation metrics were used. The evaluation accuracy, false positives, false negatives, loss,

Table 3 Performance of the proposed model compared with other models for joy, fear, anger, sadness, disgust, shame, and guilt emotion classes

Models	Joy			Fear			Anger			Sadness			Disgust			Shame			Guilt		
	P	**R**	**F1**	**P**	**R**	**F1**	**P**	**R**	**F1**	**P**	**R**	**F1**	**P**	**R**	**F1**	**P**	**R**	**F1**	**P**	**R**	**F1**
SVM	0.72	0.69	0.71	0.67	0.68	0.67	0.53	0.41	0.46	0.54	0.67	0.6	0.55	0.61	0.58	0.4	0.46	0.43	0.49	0.44	0.46
Naïve Bayes	0.47	0.63	0.54	0.49	0.57	0.53	0.55	0.23	0.33	0.32	0.5	0.39	0.36	0.4	0.38	0.09	0.31	0.13	0.34	0.28	0.3
Random Forest	0.71	0.57	0.63	0.61	0.56	0.59	0.4	0.39	0.39	0.47	0.59	0.52	0.55	0.48	0.52	0.34	0.46	0.39	0.39	0.41	0.4
Balahur *et al.*	0.43	0.47	0.45	0.48	0.55	0.51	0.35	0.41	0.38	0.7	**0.76**	0.73	0.29	0.24	0.26	0.44	0.41	0.42	0.46	0.38	0.4
Razek *et al.*	0.26	0.5	0.34	0.26	0.55	0.35	0.2	0.52	0.29	0.27	0.6	0.37	0.22	0.46	0.3	0.2	0.48	0.28	0.2	0.51	0.29
Alotaibi	0.7	0.83	0.76	0.62	0.67	0.64	-	-	-	0.73	0.73	0.73	-	-	-	**0.7**	0.55	0.62	**0.58**	0.56	**0.57**
Polignano *et al.*	0.8	0.77	0.78	0.78	0.65	0.71	**0.58**	0.52	0.55	0.64	0.66	0.65	0.6	**0.74**	0.66	0.48	0.56	0.52	0.56	0.57	**0.57**
Our Model	**0.89**	**0.94**	**0.92**	**0.89**	**0.84**	**0.86**	0.56	**0.74**	**0.64**	**0.85**	0.73	**0.78**	**0.83**	0.62	**0.71**	0.64	**0.64**	**0.64**	0.54	**0.6**	**0.57**

true negatives, and true positives were 0.6988, 98, 82, 0.8929, 141, and 1213. The classification report is highlighted in Table 2. The weighted averages for precision, recall, and the F1 score was 0.74, 0.73, 0.73, respectively.

5. Analyses of Results

Table 3 shows our proposed architecture/model against the related models acting on the ISEAR dataset. The F1 score for the proposed model was better than all the associated works, especially the current state-of-the-art in the area of emotion detection using the ISEAR dataset. It indicates the efficacy of the proposed model against the state-of-the-art [20] to the best of our knowledge.

Our model outperformed the works by [17] in terms of model accuracy, attaining an overall accuracy of 72.64%. The highest F1 score for the guilt class was shared amongst the logistic regression, *FastTextEmb*, and the proposed model. Notwithstanding the relatively low F1 scores for the anger, guilt, and shame classes, the proposed model still came out among the tops.

The work by Polignano *et al*. which used an ensemble of Bi-LSTM, convolutional neural network (CNN), and self-attention, and that of Alotaibi [7], which used a logistic regression approach slightly outperformed the proposed model in the precision metric with a difference of 0.02 and 0.06 for anger and guilt emotion classes respectively. For the sadness and disgust emotion classes, the proposed model attains the highest precision and F1 score values but succumbs to a recall value of 0.76 and 0.74 by Balahur *et al*. [21] and Polignano *et al*. [20] respectively against our model's 0.73 and 0.62 values for same emotion classes. Finally, the recall and F1 score for the guilt emotion class outperform the other models' recall and F1 scores.

6. Conclusion and Future Work

In conclusion, the paper designed a two-stage architecture based on encoders and transformers to detect fine-grained emotions from sentences, considering the context under which emotion-conveying words occurred. The result assesses the efficacy of encoder-transformers on the detection accuracy of emotions in the ISEAR dataset. It also ascertained the capabilities of BERT in extracting emotions from the ISEAR dataset. The proposed model outperformed the state-of-the-art in emotion detection on the ISEAR dataset. For all the emotion classes, the proposed model achieved better F1 scores than all other state-of-the-art models. However, since the architecture is based on BERT, it suffered from vocabulary word limitation. In the future, strategies to mitigate this limitation can be proposed to enhance the word embedding further, thus increasing the likelihood of performance for this proposed model.

References

[1] K. R. Scherer and H. G. Wallbott, "Evidence for universality and cultural variation of differential emotion response patterning.," Journal of personality and social psychology, vol. 66, no. 2, p. 310, 1994.

[2] M. Suhasini and B. Srinivasu, "Emotion detection framework for twitter data using supervised classifiers," in Data Engineering and Communication Technology, pp. 565–576, Springer, 2020.

[3] W. Ragheb, J. Az'e, S. Bringay, and M. Servajean, "Attention-based modeling for emotion detection and classification in textual conversations," arXiv preprint arXiv:1906.07020, 2019.
[4] H. Nida, K. Mahira, M. Mudasir, M. M. Ahmed, and M. Mohsin,
[5] "Automatic emotion classifier," in Progress in Advanced Computing and Intelligent Engineering, pp. 565–572, Springer, 2019.
[6] F. Mozafari and H. Tahayori, "Emotion detection by using similarity techniques," in 2019 7th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS), pp. 1–5, IEEE, 2019.
[7] F. Ghanbari-Adivi and M. Mosleh, "Text emotion detection in social networks using a novel ensemble classifier based on parzen tree estimator (tpe)," Neural Computing and Applications, vol. 31, no. 12, pp. 8971–8983, 2019.
[8] F. M. Alotaibi, "Classifying text-based emotions using logistic regression," VAWKUM Transactions on Computer Sciences, vol. 16, no. 2, pp. 31–37, 2019.
[9] F. A. Acheampong, C. Wenyu, and H. Nunoo-Mensah, "Text-based emotion detection: Advances, challenges and opportunities," Engineering Reports, vol. 2, no. 6, pp. 1–24, 2020.
[10] Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin, "Attention is all you need," in Advances in neural information processing systems, pp. 5998–6008, 2017.
[11] K. Yang, D. Lee, T. Whang, S. Lee, and H. Lim, "Emotionxku: Bert-max based contextual emotion classifier," arXiv preprint arXiv:1906.11565, 2019.
[12] [W. Antoun, F. Baly, and H. Hajj, "Arabert: Transformer-based model for arabic language understanding," arXiv preprint arXiv:2003.00104, 2020.
[13] P. Zhong, D. Wang, and C. Miao, "Knowledge-enriched transformer for emotion detection in textual conversations," arXiv preprint arXiv:1909.10681, 2019.
[14] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "Bert: Pre-training of deep bidirectional transformers for language understanding," arXiv preprint arXiv:1810.04805, 2018.
[15] B. Shmueli and L.-W. Ku, "Socialnlp emotionx 2019 challenge overview: Predicting emotions in spoken dialogues and chats," arXiv preprint arXiv:1909.07734, 2019.
[16] N. Riahi and P. Safari, "Implicit emotion detection from text with information fusion," Journal of Advances in Computer Research, vol. 7, no. 2, pp. 85–99, 2016.
[17] [Y. Li, D. McLean, Z. A. Bandar, J. D. O'shea, and K. Crockett, "Sentence similarity based on semantic nets and corpus statistics," IEEE transactions on knowledge and data engineering, vol. 18, no. 8, pp. 1138–1150, 2006.
[18] L. Singh, S. Singh, and N. Aggarwal, "Two-stage text feature selection method for human emotion recognition," in Proceedings of 2nd International Conference on Communication, Computing and Networking, pp. 531–538, Springer, 2019.
[19] Y. Yang and J. O. Pedersen, "A comparative study on feature selection in text categorization," in Icml, vol. 97, p. 35, Nashville, TN, USA, 1997.
[20] D. Seal, U. K. Roy, and R. Basak, "Sentence-level emotion detection from text based on semantic rules," in Information and Communication Technology for Sustainable Deelopment, pp. 423–430, Springer, 2020.
[21] M. Polignano, P. Basile, M. de Gemmis, and G. Semeraro, "A comparison of word-embeddings in emotion detection from text using bilstm, cnn and self-attention," in Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization, pp. 63–68, 2019.
[22] Balahur, J. M. Hermida, and A. Montoyo, "Building and exploiting emotinet, a knowledge base for emotion detection based on the appraisal theory model," IEEE Transactions on Affective Computing, vol. 3, no. 1, pp. 88–101, 2011.

PLANT DISEASE CLASSIFICATION USING TWO PATHWAY ENCODER GAN DATA GENERATION

GETINET YILMA[1], SEID BELAY[1], ZHIGUANG QIN[1*], KUMIE GEDAMU[2], MELESE AYALEW[1]

[1]Software Engineering, School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China
[2]Center for Future Media, School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China
E-MAIL: getinetyilma@gmail.com, seidatgm@gmail.com, alemugedamu@gmail.com, meleawima@gmail.com, qinzg@uestc.edu.cn

Abstract:

Deep learning is used to mitigate plant disease in early stages. Improving training sample size, feature distribution and overall sample quality impacted deep learning models correctness. In this work we proposed a generic plant disease recognition architecture with a two path way Encoder GAN data generation network. This network incorporated conditional sample generation and conditional reconstruction tasks that enabled the generation of unseen data feature. Using the tomato samples extracted from PlantVillage dataset, we were able to efficiently generate plausible images that boosted plant disease recognition. We tested the performance of our approach on popular CNN architectures such as ResNet50, GoogLeNet, VGG19 and AlexNet. The experiment result proved that the approach achieved good result both in terms of generation quality and plant disease classification performance compared to existing state of the art works. Therefore, our proposed architecture is a robust candidate for plant disease recognition.

Keywords:

Deep learning; Plant disease classification; Resnet; Two pathway encoder GAN

1. Introduction

Deep learning has been used to identify, analyze, and monitor crop health in detecting and mitigating plant diseases at the early stages[1]. Deep learning-based techniques for the automated diagnosis of plant disease have been developed with the aim of disease classification [2-5], disease segmentation[4], disease severity estimation, disease feature visualization and further analysis[8]. Due to image quality issues, collection challenges, and other factors plant disease recognition model training has faced with several difficulties.

To address training data challenges [2] and [10] used geometric transformation to augment tomato images however, it is not learning based. AR-GAN [9], [10] and [11] tried to generate high quality synthetic data to solve data scarcity for plant disease recognition. AC-GAN [12] generated high quality 128x128 pixel spatial resolution images with higher discriminability while [13] employed CR-GAN for a self-supervised learning to generate multi-view image from single view image for object and action recognition tasks. Apart from aforementioned common train dataset challenges in plant disease classification, there is also a need to generate unseen data features, improve feature distribution of generated data, introduce more controlled data generation process and guide data generation towards target feature space in order to achieve better performance. To bridge these gaps, we proposed two-pathway encoder GAN data generation model that uses sample generation and reconstruction paths which is inspired by supervised CR-GAN and auxiliary classifier loss from AC-GAN to boost plant disease classification performance.

The overall generic architecture of plant disease recognition model is shown in fig..1. Employing the potential benefit of unseen data feature in the generated data, disease classification accuracy can be boosted. The contribution of this work is (1) Provide plant disease image generation technique using Two-pathway Encoder GAN to enlarge training sample (2) Proposed generic plant disease classification architecture that combine naturalistic image generation and deep convolutional neural network architecture. (3) Evaluate the performance of the proposed approach in terms of data generation quality and classification accuracy using PlantVillage tomato dataset which is tested for the first time in this method.

2. Related Work

Data Generation and Augmentation: There are several data augmentation techniques in [2], [10] with geometric transformation to enlarge train sample lack sufficient discriminant features as they are not learning based. Mostly generated samples from GAN variants are plausible but GAN is difficult to train [14]. VAE generates blurred samples and subjected to vanishing gradient [15]. Both vanilla GAN and VAE are not either combined or have no conditional attribute for generated samples which is challenging to control the generation process. [16] presented a combined approach using VAE and GAN to generate more naturalistic images preserving discriminative features. CGAN[17] conditioned the generator and discriminator of the model with additional class attributes to direct data generation process. SGAN [18] rebuilds the class label information by the discriminator. AC-GAN [12] combined the benefit of CGAN and SGAN not only making use of class label for training, but also reconstructs the label information for every generated image and stabilizing the training process whilst learning a representation in the latent space that is independent of the class label. CR-GAN[13] is a self-supervised learning to generate multi-view image from single view image for action recognition. Encoder combined with GAN can reconstruct image feature, GAN can support plausible sample generation and conditioning their combined effort helps to control the generation process towards the target feature. Therefore, we proposed two-pathway encoder GAN data generation model that uses sample generation and reconstruction paths inspired by supervised CR-GAN and auxiliary classifier loss from AC-GAN to boost plant disease classification performance.

Classification: There are several convolutional neural network architectures used for crop disease classification using plant village dataset with several experimental setting as stated in [1] used AlexNet, GoogLeNet with and without transfer learning, other disease recognition works in [2],[19],[3], [20] , and [21] demonstrated performance of different CNN architectures. In addition summary of plant disease detection as reviewed in [4] [4] is also presented with details. PlantDiseaseNet [10] architecture proposed PDNet-1 for leaf detection by species and PDNet-2 disease classification. PlantDiseaseNet still needs more data with sufficient detail to improve disease recognition. Papers [1], [4], [5] , [10], [19] use deep CNN architectures ResNet, AlexNet, GoogLeNet and VGG for plant disease recognition performing best when supported by massive but diverse training data.

The present approach has not been achieving a promising result due to data set feature distribution for training deeper models, homogeneity in data quality, train sample size, and the reduced testing time accuracy. Therefore, we proposed a deep generative model based on two pathway Encoder GAN to enlarge training set sample to improve the performance of plant disease classification.

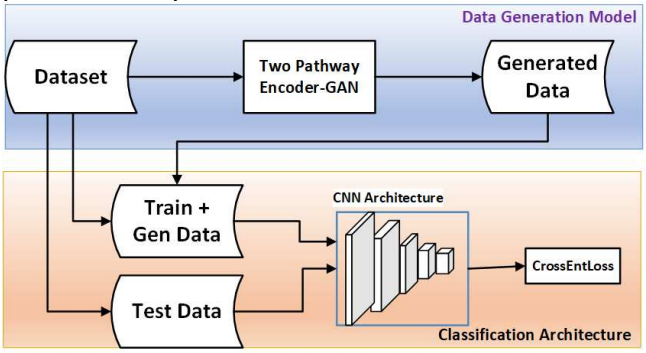


Fig.1 Disease classification architecture

3. Proposed Method

Data Generation and Augmentation: In this work we proposed Two-pathway encoder GAN for data generation task as shown in Fig.2. This data generation approach has two explicit paths. The first path exhibits the conditioned GAN characteristics which is the generation path (Generator-discriminator) G_z tries to generate from noise z. The second path exhibits the Encoder GAN a.k.a reconstruction path, i.e. Encoder-Generator followed by Discriminator which tries to reconstruct image feature at pixel level. The two pathway encoder GAN offers a high resolution data generation for better discriminability, extract unseen data feature with the help of noise and conditional generation (G_z) process. In generation pathway Generator $G_z(z,d)$ takes random noise z and disease class label d to generate an image gen_z. Then in the reconstruction pathway the Encoder $E(x)$ receives train image x to produces encoded latent feature space $\bar{z}$ and estimated class label $\bar{d}$. The latent space $\bar{z}$ and label d are used as input to Encoder-Generator $G_{\bar{z}}$ ($\bar{z}$,d). The discriminator D_s discriminates the real data samples from synthetic. Simultaneously, it encourages the G_z and E to fit the true distribution by minimizing the loss for both networks. The $G_{\bar{z}}$ acts as a decoder network which takes optimized output from E and so it is not directly optimized by D rather indirectly through the E network. The G_z and E use the discriminator's loss information to generate plausible images so that their generation sufficiently fools the discriminator network.

The two generators G_z and $G_{\bar{z}}$ share a single disease class label d to guide the training towards a common feature. The approach is formulated as follows Generation from

random noise, the G_z takes in a random noise z and one hot vector class label d as input to generates an image gen_z. Then the task of D network is to minimize loss from G_z and gradient penalty for stable GAN training as used in [22]. D is minimized as,

$$\begin{aligned} &E_{z\sim p_z}\left[D_s\left(G_z(z,d)\right)\right] - E_{x\sim p_x}\left[D_s(\mathrm{x})\right] \\ &+\lambda_1 E_{\hat{x}\sim p_{\hat{x}}}\left[\left(||\nabla_{\hat{\mathrm{x}}} D(\hat{\mathrm{x}})||_2 - 1\right)^2\right] \\ &-\lambda_2 E_{x\sim p_x}\left[D_d(x) = d\right] \end{aligned} \quad (1)$$

where z denote random noise and z is true data, d refers to disease class label, $\mathrm{p_z}$ and $\mathrm{p_x}$ refers to the noise and true data distribution, respectively. The loss from D is maximized by the generator to fool the discriminator through the equation,

$$E_{z\sim p_z}\left[D_s\left(G_z(z,d)\right)\right] + \lambda_2 E_{z\sim p_z}\left[P\left(D_d\left(G_z(d,z)\right) = d\right)\right] \quad (2)$$

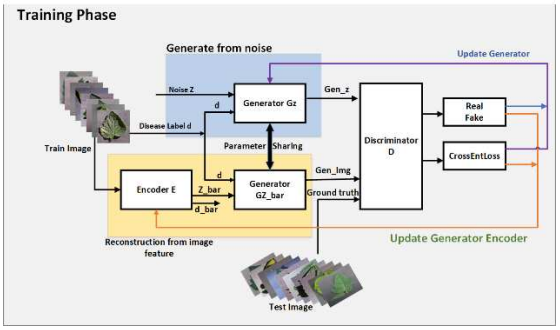


Fig.2 Two pathway Encoder GAN data generation training phase.

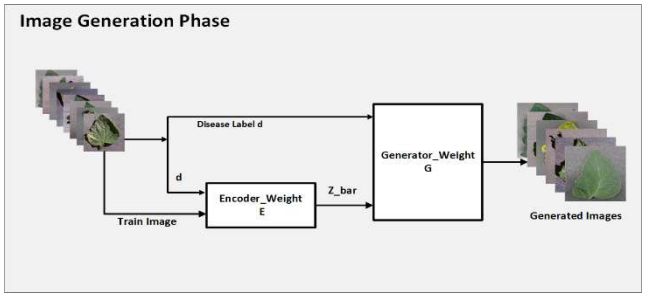


Fig.3 Two pathway Encoder GAN image generation phase.

From the reconstruction E takes a sample train image x produces latent vector $\bar{z}$ and estimated class label $\bar{d}$ as output. The **generator** takes in $\bar{z}$ from the E network and shared class label d to generate an image Gen_img as shown in fig..2, so D minimizes eqn. (1) and E helping Gz_bar by maximizing,

$$E_{x_i, x_j\sim p_x}\begin{bmatrix} \mathrm{D_s}\left(\tilde{\mathrm{x}}_\mathrm{j}\right) + \lambda_2 \mathrm{P}\left(\mathrm{D_d}\left(\tilde{\mathrm{x}}_\mathrm{j}\right) = \mathrm{d_j}\right) - \lambda_3 \mathrm{L_1}\left(\tilde{\mathrm{x}}_\mathrm{j}, \mathrm{x_j}\right) \\ -\lambda_2 (E(\mathrm{x_i}), \mathrm{d_i}) \end{bmatrix} \quad (3)$$

where λ_1=10, λ_2=1 and $\lambda_3 = 0.01$ are the constant values to control the relative loss weight in the objective function and are recommendation from WGAN-GP[22]. $\mathrm{L_1}$ loss is used to compute pixel wise distance loss. Once the generation network was trained, a new synthetic sample that enlarge the training set were generated by the generation phase as shown in fig..3.

Disease Classification: For the purpose of disease classification deep CNN architectures such as ResNet, AlexNet, VGG and GoogLeNet are commonly popular CNN architectures. These models are suggested as the most frequently used architectures in [19] based on the performance score in different works. As shown in fig.1 the data generation section enlarges training sample size and classification part handles plant disease recognition. For our work we employed ResNet50, AlexNet, VGG19 and GoogLeNet architectures for plant disease classification task. Our approach we used similar train and test data split, parameter settings and softmax cross entropy loss with Adam optimizer to train the classifiers. The classification loss is as defined in eqn. 4.

$$\begin{aligned} \bar{y}_c &= \frac{\exp\left(wF(X_t, \Theta_f)\right)}{\sum_k \exp\left(wF(X_k, \Theta_f)\right)} \\ \bar{y} &= \{\bar{y}_1, \bar{y}_2 \ldots\ldots \bar{y}_c\} \\ &= -y \log(\bar{y}) \end{aligned} \quad (4)$$

Where $\bar{y}$ is predicted class probability, $wF(X_t, \Theta_f)$ is the soft max function

Generation assessment: To investigate the quality of generated images comparing with the real image we used CW-SSIM [23] assessment method. This method is robust and tolerant to geometric distortion such as rotation, translation and scaling [23]. Therefore, CW-SSIM, used to measure quality of generated image CW-SSIM as in eqn. (5).

$$\begin{aligned} &CW - SSIM(x_{di}, \bar{x}_{di}) = \\ &\frac{1}{N}\sum_{n=1}^{N} \frac{2\left|\sum_{m=1}^{M} x_{di}(m)\bar{x}_{di}(m)\right| + k}{\sum_{m=1}^{M}\left|x_{di}(m)\right|^2 + \sum_{m=1}^{M}\left|\bar{x}_{di}(m)\right|^2 + k} \end{aligned} \quad (5)$$

Where x_{di} the ground truth image in disease class di, $\bar{x}_{di}$ is the generated image, k is small constant for function stability.

4. Dataset and Experiment setting

To demonstrate the applicability of our approach, we conducted experiments for data generation and plant disease classification. Generally, to enlarge the train data we used two additional approaches for comparison 1) Built in data augmentation using transformation functions: zoom, rotate, flip_left_right, zoom random, and shear functions. 2) CGAN is used to generate synthetic images using class label d as a condition variable, 50% train and 50% test split was used for training the model.

Dataset: The tomato image in PlantVillage [4] dataset is extracted for experiment because of more no of classes than other plant types in the dataset. It has 256x256 spatial resolution,18154 images, 10 classes among which nine classes unhealthy and one class healthy also described in table 1 and fig.4 below.

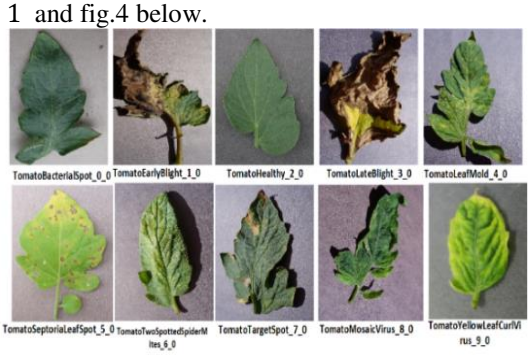


Fig.4 Sample mages and classes showing disease name, disease class and image sequence number.

Table 1 Tomato dataset showing class information, number of train-test split and number of generated images.

Target Name	Train	Test	Generated
BacterialSpot_0	1064	1064	1064
EarlyBlight_1	500	500	500
Healthy_2	796	796	796
LateBlight_3	955	955	955
LeafMold_4	476	476	476
SeptoriaLeafSpot_5	886	886	886
TwoSpottedSpiderMites	838	838	838
TargetSpot_7	702	702	702
MosaicVirus_8	187	187	187
YellowLeafCurlVirus_9	2679	2679	2679
	9077	9077	9077

Implementation Details: GPU GForce GTX 2080Ti, 11GB memory and Pytorch framework. using Adam optimizer where learning rate 1*e-4, batch size 32 and epoch 100 was used to train the generation. For classification network Adam optimizer, initial learning rate of 1*e-1 with batch size 16, and a total of 50 epochs were used.

5. Discussion

Data generation Assessment: To demonstrate the data generation, we conducted three experiments with the same experimental configuration, the same data source, and data split 50% for train 50% for test. We also compared our approach with CGAN and auto augmented data in terms of CW-SSIM [23] value and classification accuracy.

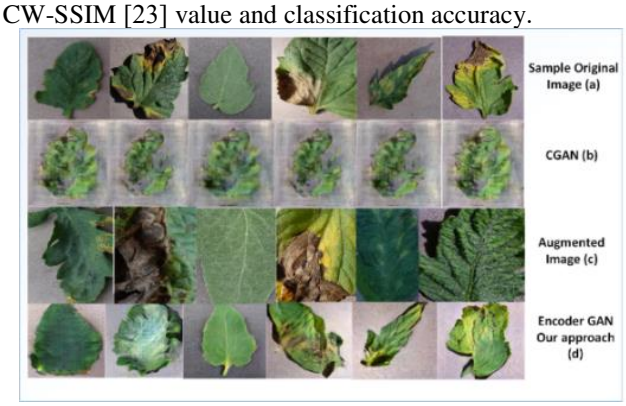


Fig.5 Sample images (a) original dataset, (b) generated using CGAN, (c) augmented using built in transformation functions and, (d) generated from proposed approach

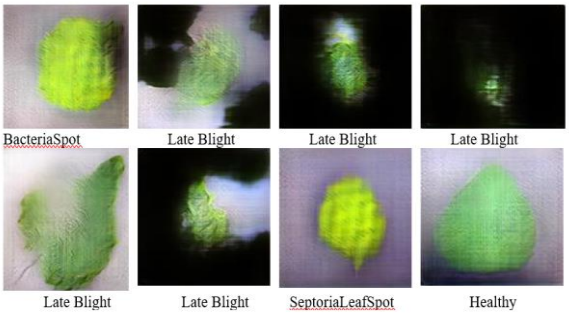


Fig.6 Failed images generated by the proposed approach. This is due to size of the image, the disease behavior on the leaves and the leaf background color.

To investigate the quality of generated images comparing with the true data as displayed in fig.5 visually the CGAN generation (b) produced blurry samples that failed to clearly show disease spots, the augmentation (c) generated clear images when seen visually but cropped some parts of the image deforming the whole sample structure, two pathway Encoder GAN (d) has produced better quality than CGAN and less quality than augmentation when inspected visually. CW-SSIM is a robust quantitative method which is tolerant to geometric distortion such as rotation, translation and scaling.

Shown in table 2 For CGAN and augmented generated images the CW-SSIM values are smaller than the proposed approach.

Table 2 CW-SSIM quality assessment for generated images compared with the ground truth images for each class

Class	0	1	2	3	4	5	6	7	8	9
CGAN	68.7	69.7	51.3	68.4	65.0	67.2	71.3	69.3	65.3	67.4
Aug	78.5	74.3	59.3	71.5	66.9	70.0	72.5	65.2	65.8	69.5
Ours	**83.1**	**85.7**	**77.0**	**83.8**	**83.2**	**84.5**	**83.9**	**84.2**	**81.2**	**87.3**

The average CW-SSIM for our approach for each class is above 83% and higher than other approaches, this reveals the plausibility of the generated image for disease recognition.

Table 3 Tomato disease classification accuracy via data generation for selected CNN architectures in %

CNN Arch	W/t	Aug	CGAN	Ours
AlexNet	87.25	88.25	87.86	87.97
GoogLeNet	91.47	96.36	92.38	96.98
VGG19	92.29	96.13	85.19	98.04
ResNet50	93.02	97.41	91.01	**98.74**

Plant Disease Classification Assessment: As given in table 3 and fig.7 we have compared classification results from four CNN architectures ResNet50, AlexNet, GoogLeNet, and VGG19 to verify the generated data contribution towards disease recognition accuracy. From the table, we can see that data generation outperformed when compared with the data without generation. Except CGAN other two generation methods contributed discriminative feature towards classification accuracy. Data generation based on the proposed approach has produced improved the model performance. Among the trained models ResNet50 scored the best result **98.74**%.

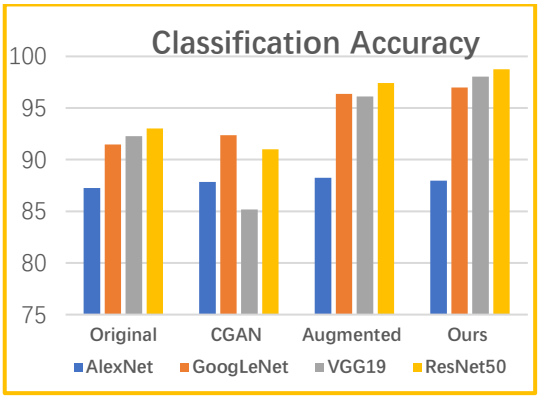


Fig.7 Classification accuracy comparison between CNN architectures across data settings

Comparison with state of the art works: for the purpose of comparison, we have presented three works which have similar dataset source and focusing deep learning technique.

Table 4 Experiment configuration for training tomato disease classification via data generation in %

Author	Method	Dataset	Accu
[2]	ResNet	9 classes, 5550 images	97.28
[21]	SCRNN	9 classes, 18,148 images	90
[20]	AlexNet	10 classes, 18,148	95.65
Ours	**ResNet50**	**10 classes, 18,160**	**98.74**

The table 4 shows different authors use methods such as ResNet50, SCRNN and AlexNet deep learning architectures for classification on tomato images extracted from PlantVillage dataset. The author [20] had similar dataset configuration with our dataset, but [2] and [21] had different preprocessing, number of images, and parameters. Disease classification state of the art result comparison using the same data source PlantVillage[4] tomato dataset, our approach has a score **98.74%** accuracy where as others are below the proposed approach. This demonstrates classification via the proposed data generation approach boosts training accuracy.

6. Conclusion

Training deeper networks require more diverse, balanced and massive amount of training data for preventing the risk of model overfitting and boost performance of disease classification. In this paper we used two pathway encoder GAN, built in data augmentation functions and CGAN data generation techniques to expand training data in an attempt to solve dataset related issues. The two pathway encoder GAN has enabled generation of more plausible image than other approaches. Two pathway Encoder GAN data generation enabled both to enlarge training data and construct unseen data feature hence, prevented model overfitting and boosted training accuracy. With the proposed generic architecture plant disease recognition model outperformed the state of the art works. We also recommend that this work can be extended to semi supervised or unsupervised technique.

Acknowledgements

This work was supported by National Natural Science Foundation of China (NSFC), University of Electronic Science and Technology of China, under project Privacy & Security key theory and Technology based on Data Cycle (Grant No 61520106007).

References

[1] S. P. Mohanty, D. P. Hughes, and M. Salathé, “Using deep learning for image-based plant disease detection,” Front. Plant Sci., vol. 7, no. September, pp. 1–10, 2016.

[2] K. Zhang, Q. Wu, A. Liu, and X. Meng, “Can deep learning identify tomato leaf disease?,” Adv. Multimed., vol. 2018, 2018.

[3] M. Brahimi, K. Boukhalfa, A. Moussaoui, and M. Brahimi, “Deep Learning for Tomato Diseases : Classification and Symptoms Visualization Deep

Learning for Tomato Diseases : Classification and Symptoms Visualization," Appl. Artif. Intell., vol. 31, no. 4, pp. 299–315, 2017.
[4] A. Kamilaris and F. X. Prenafeta-Boldú, "Deep learning in agriculture: A survey," Comput. Electron. Agric., vol. 147, no. July 2017, pp. 70–90, 2018.
[5] M. H. Saleem, J. Potgieter, and K. M. Arif, "Plant disease detection and classification by deep learning," Plants, vol. 8, no. 11, pp. 32–34, 2019.
[6] R. Barth, J. IJsselmuiden, J. Hemming, and E. J. Van Henten, "Synthetic bootstrapping of convolutional neural networks for semantic plant part segmentation," Comput. Electron. Agric., vol. 161, no. July, pp. 291–304, Jun. 2019.
[7] Q. H. Cap, H. Uga, S. Kagiwada, and H. Iyatomi, "LeafGAN: An Effective Data Augmentation Method for Practical Plant Disease Diagnosis," Feb. 2020.
[8] M. Brahimi, M. Arsenovic, S. Laraba, S. Sladojevic, K. Boukhalfa, and A. Moussaoui, Deep Learning for Plant Diseases: Detection and Saliency Map Visualisation. Springer International Publishing, 2018.
[9] H. Nazki, S. Yoon, A. Fuentes, and D. S. Park, "Unsupervised image translation using adversarial networks for improved plant disease recognition," Comput. Electron. Agric., vol. 168, no. 1, 2020.
[10] M. Arsenovic, M. Karanovic, S. Sladojevic, A. Anderla, and D. Stefanovic, "Solving current limitations of deep learning based approaches for plant disease detection," Symmetry (Basel)., vol. 11, no. 7, 2019.
[11] H. Nazki, J. Lee, S. Yoon, and D. S. Park, "Image-to-Image Translation with GAN for Synthetic Data Augmentation in Plant Disease Datasets," Korean Inst. Smart Media, vol. 8, no. 2, pp. 46–57, 2019.
[12] A. Odena, C. Olah, and J. Shlens, "Conditional image synthesis with auxiliary classifier gans," 34th Int. Conf. Mach. Learn. ICML 2017, vol. 6, pp. 4043–4055, 2017.
[13] Y. Tian, X. Peng, L. Zhao, S. Zhang, and D. N. Metaxas, "CR-GAN: Learning complete representations for multi-view generation," IJCAI Int. Jt. Conf. Artif. Intell., vol. 2018-July, pp. 942–948, 2018.
[14] K. Lata, M. Dave, and N. K.N., "Data Augmentation Using Generative Adversarial Network," SSRN Electron. J., pp. 1–14, 2019.
[15] L. Wan, J. Wan, Y. Jin, Z. Tan, and S. Z. Li, "Fine-grained multi-attribute adversarial learning for face generation of age, gender and ethnicity," Proc. - 2018 Int. Conf. Biometrics, ICB 2018, pp. 98–103, 2018.
[16] J. Bao, D. Chen, F. Wen, H. Li, and G. Hua, "CVAE-GAN: Fine-Grained Image Generation through Asymmetric Training," Proc. IEEE Int. Conf. Comput. Vis., vol. 2017-Octob, pp. 2764–2773, 2017.
[17] S. O. M. Mirza, "Conditional Generative Adversarial Nets," arXiv Prepr. arXiv1411.1784, 2014.
[18] A. Odena, "Semi-Supervised Learning with Generative Adversarial Networks," pp. 1–3, 2016.
[19] K. P. Ferentinos, "Deep learning models for plant disease detection and diagnosis," Comput. Electron. Agric., vol. 145, no. January, pp. 311–318, 2018.
[20] H. Durmus, E. O. Gunes, and M. Kirci, "Disease detection on the leaves of the tomato plants by using deep learning," in 2017 6th International Conference on Agro-Geoinformatics, Agro-Geoinformatics 2017, Aug. 2017.
[21] K. Yamamoto, T. Togami, and N. Yamaguchi, "Super-resolution of plant disease images for the acceleration of image-based phenotyping and vigor diagnosis in agriculture," Sensors (Switzerland), vol. 17, no. 11, pp. 1–13, 2017.
[22] I. Gulrajani, F. Ahmed, M. Arjovsky, V. Dumoulin, and A. Courville, "Improved training of wasserstein GANs," Adv. Neural Inf. Process. Syst., vol. 2017-Decem, pp. 5768–5778, 2017.
[23] I. I. Conference and I. Processing, "CW-SSIM BASED IMAGE CLASSIFICATION Yang Gao , Abdul Rehman and Zhou Wang," pp. 1249–1252, 2011.

EFFICIENT TRANSFER LAERNING USED IN THE CLASSIFICATION OF GASTROSCOPIC IMAGES WITH SMALL DATASET

DU WENJU[1, 2], RAO NINI[1, 2], WANG YINGCHUN[1, 2], HU DINGCAN[1, 2], YONG JIAHAO[1, 2]

[1] Center for Informational Biology, University of Electronic Science and Technology of China, Chengdu 610054, China
[2] School of Life Science and Technology, University of Electronic Science and Technology of China, Chengdu 610054, China
E-MAIL: aduwenju@163.com, raonn@uestc.edu.cn, 18830202078@163.com, 1641166080@qq.com, 986903165@qq.com

Abstract:

Deep learning (DL) has gained success in image classification. However, DL always needs a large number of labeled training data which are not usually available for gastroscopic image analysis. Therefore, the pre-trained convolutional neural networks (CNNs) models are important. The transfer learning (TL) method could leverage the pre-trained model in natural images to gastroscopic images. In this paper, we have studied different TL methods on small dataset of gastroscopic images. We have fine-tuned the current deep CNNs: EfficientNet, ResNet and DenseNet on three kinds of gastroscopic images from kvasirv2 dataset. The results demonstrated that the pre-trained models of current deep CNNs can get considerable classification results on gastroscopic images with small dataset.

Keywords:

Gastroscopic image; Classification; Deep learning; Transfer learning; Lesion

1. Introduction

Deep learning (DL) has gained success in image classification. However, DL always needs a large number of labeled training data which are not always available for gastroscopic image analysis. Therefore, the pre-trained convolutional neural networks (CNNs) models are important. Many exploring works of transfer learning (TL) method on gastroscopic images have been carried out by the researchers. Liu *et al.* [1] proposed a TL framework by fine-tuning the pre-trained CNNs to classify gastric narrow-band imaging images into three classes: chronic gastritis, low grade neoplasia and early gastric cancer. They fine-tuned four CNNs: VGG16 [2], InceptionV3 [3], ResNet50 [4] and InceptionResNetV2 [5], and they got the best classification result from ResNet50. Similarly, Van Riel *et al.* [6] also applied the TL method based on the current popular CNNs such as AlexNet, VGGNet, and GoogLeNet, to build an esophageal cancer detection and annotation method. Ohmori *et al.* [7] fine-tuned the single shot detector (SSD) [8] and realized the detection and differentiation of esophageal squamous cell carcinoma lesions (ESCC). Kumagai *et al.* [9] developed an AI diagnosis system based on the TL via GoogLeNet, which can classify malignant (ESCC) and non-cancerous lesions in endocytoscopic system images. Zhu *et al.* [10] constructed a CNN computer-aided detection system based on gastroscopic images to determine gastric cancer invasion depth and screen patients for endoscopic resection. This fully demonstrates the powerful capabilities of TL.

Although TL method has showed its powerful capabilities on the classification of gastroscopic images, there is still lack of the works that exploring more about which TL method is more efficient. What's more, the above works only focused on the classification of esophageal or gastric lesions, none of them simultaneously focused on both esophageal and gastric lesions. As we all known that the esophageal and gastric images were all collected by gastroscopy from a clinical examination. Thus, the doctor usually diagnosis these gastroscopic images including esophagus and stomach at one time. In other words, if we can develop a CNN model that could classify esophageal and gastric lesions gastroscopic images at the same time, this algorithm would be with more application prospects. In this work, we developed a multi-classification method on both esophageal and gastric images based on TL of current deep CNNs. We studied different TL methods on small dataset. We fine-tuned the current deep and efficiency CNNs: EfficientNet [11], ResNet and DenseNet [12] on three kinds of gastroscopic images from kvasirv2 dataset. We also explored the effect of different TL methods on the training process and the classification results. We found that fine-tuning all the layers of the CNNs is more efficient, and we got the best classification results from fine-tuning ResNet152.

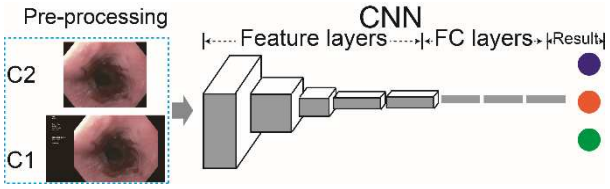


Fig.1 Structure of the classification method

2. Materials and methods

2.1. Materials

Three classes of gastroscopic images with high resolution, including normal z-line, esophagitis and normal pylorus were downloaded from kvasirv2 database [13], with 1000 images for each class. All the z-lines and esophagitis lesions can be seen clearly in the kvasirv2 images, and the mucous membrane of normal pylorus can be seen very clearly. Each class of images were randomly split to three groups: train, validation and test groups with the ratio of 60%, 20% and 20% respectively. In other words, there are 600, 200 and 200 images in the training, validation and testing groups.

In this work, the programming language implemented is python 3.6.4, and the deep learning framework is PyTorch 1.0.0 (https://pytorch.org/). All the experiments were performed on a server based on Uuntu 16.04.6 LTS (GNU/Linux 4.8.0-36-generic X86_64) and equipped with four graphics processing units of Nvidia GeForce RTX 2080 Ti, 10989 MiB.

2.2. Methods

The main steps of the proposed method are shown in Figure 1. The pre-proposing step was first performed to remove the black background regions of gastroscopic images. Then the image augmentation method was performed to increase the data scale and diversity. Next, the augmented images were send to the fine-tuned CNN. After several epochs training and validating, the final classification results for three classes of gastroscopic images were obtained. The details of the above steps are systematically described as follows.

2.2.1. Pre-processing

Most of the gastroscopic images include large areas of black background regions (as shown in C1 of Figure 1) which are useless areas for lesion identification, so we firstly cropped these regions through a window with fixed size [14], as shown in C2. Then a series of data augmentation operations including uniformly resized to 224×224, random horizontal flip and random affine were carried out on C2.

2.2.2. Classification of gastroscopic images using transfer learning method

After pre-processing, the pre-processed images were sent to a fine-tuned CNN. In the fine-tuning steps, the FC layers of the original CNN were removed and replaced by three new FC layers which changed the output categories to N (N=3).

There are mainly three ways of TLs: only fine-tuning the FC layers in the former 20 epochs, then fine-tuning all the layers in the left 80 epochs (TL-1); fine-tuning all the layers from the beginning (TL-2); only fine-tuning the last FC layers (TL-3) [15].

In all the experiments, the training epochs were set to 100, learning rate (Lr) as 0.005.

3. Experiments and results

In order to find the more efficient CNN and better TL method, we designed some comparison experiments.

3.1. Metrics

The accuracy (Acc), recall (Rec), precision (Pre) and F1-score (F1) were used to evaluate the classification oerformance of each method, as shown in equations (1)-(4).

$$\mathrm{Acc} = \frac{\sum_i n_{i,i}}{\sum_{i,j} n_{i,j}} \tag{1}$$

$$\mathrm{Pr}_j = \frac{n_{j,j}}{\sum_j n_{i,j}} \tag{2}$$

$$\mathrm{Rec}_i = \frac{n_{i,i}}{\sum_i n_{i,j}} \tag{3}$$

$$\mathrm{F1}_j = \frac{2 \times \mathrm{Pr}_j \times \mathrm{Re}c_j}{\mathrm{Pr}_j + \mathrm{Re}c_j} \tag{4}$$

where i,j refers to the index of each disease, $n_{i,j}$ indicates the number of the disease i predicted as j. Similarly, $n_{i,i}$ and $n_{j,j}$ refers to the number of disease i and j predicted as i and j, respectively. Acc and F1 evaluate the comprehensive classification abilities. Pr represents the precision rate of the disease recognition. Rec represents the sensitivity.

3.2. Comparison among three transfer learning methods

We designed a validation experiment among three TL

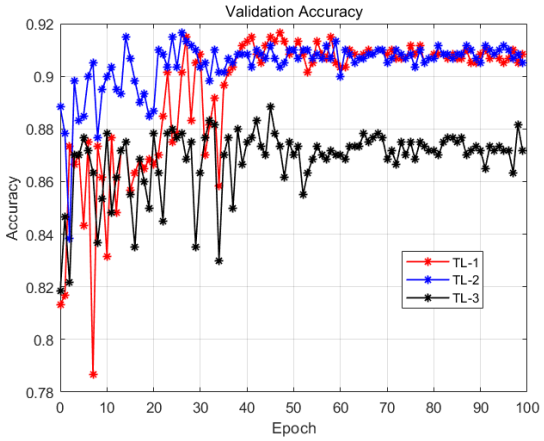


Fig.2 Comparison of validation accuracy between three transfer learning methods during training process.

Table 1 Comparison of classification results.

Metrics	Method	z-line	esophagitis	pylorus	Acc
Pre	TL-1	0.8293	0.8505	0.9950	0.8917
	TL-2	**0.8133**	**0.9029**	**1.0000**	**0.9017**
	TL-3	0.7333	0.7592	1.0000	0.8300
Rec	TL-1	0.8500	**0.8250**	1.0000	
	TL-2	**0.9150**	0.7900	**1.0000**	
	TL-3	0.7700	0.7250	0.9950	
F1	TL-1	0.8395	0.8376	0.8395	
	TL-2	**0.8612**	**0.8427**	**0.8612**	
	TL-3	0.7512	0.7417	0.7512	

methods to explore which TL method is more efficient. The validation accuracy (denoted by val-acc) changes with training epochs (Figure 2 and Table 1), where TL-1, TL-2 and TL-3 correspond to the three TL methods as described in section 2.2.2. It can be seen from Figure 1 that the val-acc of TL-2 method increased faster at the first 20 epochs, then the val-acc of TL-1 method raised to be almost the same with TL-1 in the 20-50 epochs. In the left 50-100 epochs the val-acc curves of TL-1 and TL-2 were intertwined and the val-accs were saturated. The TL-3 method performed the worst. We further compared the test accuracies between three TL methods and the results can be seen in Table 1, where the optimal values were bolded. In summary, TL-2 method was more efficient.

3.3. Comparison among three state-of-the art CNNs

We compared the classification performances of ResNet152, DenseNet161 and EffiocientNet-b7 via TL, and the Pre, Rec, F1 and Acc on the test dataset were shown in Table 2. The optimal values of each evaluated parameters were bolded, which revealed that ResNet152 was the best. However, the gaps of the classification results among three CNNs were small. The overall classification accuracy of ResNet152 was only 0.0067 higher than DenseNet161.

Table 2 Classification performance of three CNNs with TLs.

Metrics	CNNs	z-line	esophagitis	pylorus	Acc
Pre	Res152	0.8133	**0.9029**	**1.0000**	**0.9017**
	Den161	0.8216	0.8757	0.9901	0.8950
	E-b7	**0.8504**	0.8778	1.0000	0.8917
Rec	Res152	**0.9150**	0.7900	**1.0000**	
	Den161	0.8750	**0.8100**	1.0000	
	E-b7	0.8456	0.7900	0.9950	
F1	Res152	**0.8612**	**0.8427**	**1.0000**	
	Den161	0.8475	0.8416	0.9950	
	E-b7	0.8456	0.8316	0.9975	

Note: Res152=ResNet152; Den161=DenseNet161; E-b7=EfficientNet-b7

Table 3 Comparison of classification results between different EfficientNets

CNN	Acc	M-Pre	M-Rec	M-F1
E-b0	0.8833	0.8837	0.8833	0.8831
E-b1	0.8867	0.8867	0.8867	0.8865
E-b2	0.8833	0.8855	0.8833	0.8829
E-b3	0.8800	0.8801	0.8800	0.8794
E-b4	0.8900	0.8908	**0.8900**	0.8899
E-b5	0.8850	0.8863	0.8850	0.8848
E-b6	0.8850	0.8899	0.8850	0.8846
E-b7	**0.8917**	**0.8944**	0.8769	**0.8916**

Note: E-bi=EfficientNet-bi, i=0,1,…,7; M-Pre=Mean Pre; others are the same.

The effect on more complex and deeper CNNs were further studied by comparing the classification results between different EfficientNets. As ResNet and DenseNet were well known and had been well studied, and EfficientNet was new to us, so the EfficientNet was selected. We trained EfficientNet-b0 to EfficientNet-b7 on the three kinds of gastrpscopic images and tested all the EfficientNets on the test dataset. The comparison results were shown in Table 3, which shows the performance of Efficient-b7 was the best. However, the gaps of each EfficientNets' classification results were quite small. For instance, the overall classification accuracy of E-b0 and E-b2, E-b5 and E-b6 were the same. This indicated that the classification ability of deep and complex CNNs via TL on the small gastroscopic dataset used in this work was saturated.

In summary, the TL methods of current state-of-the-art deeper CNNs have saturated on the small dataset used in this work, and the overall classification results would be almost the same no matter which deep CNN was used. More images were needed for better classification results.

4. Conclusions

In this paper, we proposed a gastroscopic image classification method by fine-tuning three current deeper and efficient CNNs: EfficientNet, ResNet and DenseNet. We found that the best results can be gotten by fine-turning all the layers of ResNet152, and the classification results of deep CNNs on the small gastroscopic dataset used in this work were almost saturated.

Acknowledgements

This work was supported in part by the National Natural Science Foundation of China under Grant 61872405 and Grant 61720106004, and in part by the Key R&D Project of Sichuan Province (2020YFS0243).

References

[1] X. Liu, C. Wang, J. Bai, and G. Liao, "Fine-tuning Pre-trained Convolutional Neural Networks for Gastric Precancerous Disease Classification on Magnification Narrow-band Imaging Images," Neurocomputing, vol. 392, pp. 253–267, June. 2020.

[2] K. Simonyan and A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Images Recognition," Proceeding of International Conference on Learning Representations (ICLR), Banff, Canada, pp. 1-14, April 2014.

[3] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the Inception Architecture for Computer Vision," Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Las Vegas NV,USA, pp. 2818–2826, June 2016.

[4] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Las Vegas NV,USA , pp. 770–778, June 2016.

[5] C. Szegedy, S. Ioffe, V. Vanhoucke, and A. Alemi, "Inception-v4, Inception-ResNet and the Impact of Residual Connections on Learning," Proceeding of AAAI Conference on Artificial Intelligence, San Francisco, California USA, pp. 4278-4284 February 2017.

[6] S. Van Riel, F. Van Der Sommen, S. Zinger et al., "Automatic detection of early esophageal cancer with CNNS using transfer learning," Proceedings of International Conference on Image Processing, ICIP, Athens, Greece , pp. 1383–1387, October 2018.

[7] M. Ohmori, R. Ishihara, K. Aoyama et al., "Endoscopic detection and differentiation of esophageal lesions using a deep neural network," Gastrointest. Endosc., vol. 91, no. 2, pp. 301-309.e1., Sep. 2020.

[8] W. Liu, D. Angulelov, D. Erhan et al., "SSD: Single shot multibox detector," Proceeding of European conference on computer vision, ECCV, Amsterdam, The Netherlands, pp. 21–37, October 2016.

[9] Y. Kumagai, K. Takubo, K. Kawada et al., "Diagnosis using deep-learning artificial intelligence based on the endocytoscopic observation of the esophagus," Esophagus, vol. 16, no. 2, pp. 180–187, Dec. 2019.

[10] Y. Zhu, Q. Wang, M. Xu al., "Application of convolutional neural network in the diagnosis of the invasion depth of gastric cancer based on conventional endoscopy," Gastrointest. Endosc., vol. 89, no. 4, pp. 806-815.e1,Nov. 2018.

[11] M. Tan and Q. V. Le, "EfficientNet: Rethinking model scaling for convolutional neural networks," 36th Int. Conf. Mach. Learn. ICML 2019, Long Beach, pp. 10691–10700, June 2019.

[12] G. Huang, Z. Liu, L. Van Der Maaten, and K. Q. Weinberger, "Densely connected convolutional networks," Proceeding of 30th IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017, Honolulu, Hawaii, pp. 2261–2269.

[13] K. Pogorelov, P. Schmidt, M. Riegler et al., "Kvasir: A Multi-Class Image Dataset for Computer Aided Gastrointestinal Disease Detection," Proc. 8th ACM Multimed. Syst. Conf. - MMSys'17, Taipei Taiwan, China, pp. 164–169, June 2017.

[14] D. Liu, T.Gan, N. Rao et al., "Identification of lesion images from gastrointestinal endoscope based on feature extraction of combinational methods with and without learning process," Med. Image Anal., vol. 32, pp. 281–294, Aug. 2016.

[15] W. Du, N. Rao, D. Liu et al., "Review on the Applications of Deep Learning in the Analysis of Gastrointestinal Endoscopy Images," IEEE Access, vol. 7, pp. 142053–142069, Oct. 2019.

SEMANTIC DEPENDENCY WORD REPRESENTATION

CHONG FU[1], HANG ZHAO[2], SHUTAO ZHANG[3], LINJING ZHOU[4]

School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China
E-MAIL: fuc@uestc.edu.cn

Abstract:

We provide a novel model architecture for learning Chinese word representations with semantic dependency information. These representations can solve two problems, the first is to avoid polysemy, the second is to capture remote features. Our representations are learned from a Chinese semantic dependency model and a normal word embedding model (e.g.,CBOW or Skip-gram). Using CBOW or Skip-gram model, the word representations can get some semantic information from the position of words. Semantic dependency model can find different word pairs in the sentence and predict the semantic relationship between each word pair.The first word of each word pair represents the current word, and the second word represents the target word. By fusing the semantic information after semantic analysis into the basic word representations, we can get more accurate and dynamic word representations. More importantly, we have achieved advanced results when we use these word representations in sentiment classification task and subject classification task.

Keywords:

Word representation; Semantic dependency; Feature fusion; Sentiment classification; Subject classification

1. Introduction

Pre-trained word representations are important to many nature language processing tasks. Mikolov et al. has provided methods for learning word representations in [1] and [2]. However, the quality of word representations by these methods is not high enough. The following are two reasons: (1) the same word can only be mapped to a fixed vector space in different contexts, which will lose a lot of key information, (2) due to the limitation of window size, the model cannot fully capture the relationship between long-distance words, resulting in the loss of long-distance features. In this paper, we propose a new method to generate word representations, which contain rich semantic dependency information and solve the above problems well. Our word representations can be easy to use before other existing models and can significantly improve the performance of downstream tasks.

Our representations add more semantic information to the traditional word vector representations in [1]. We use the semantic dependency parser in [3] to express a sentence as many pairs of related words and the dependency between each pair. The word representation we proposed is formed by the fusion of these semantic dependency information and the traditional word representation. For this reason, we call them SDE (Semantic Dependency Embedding).

The dependent (the first word in a word pair) and the head (the second word in a word pair) can enrich semantic information and strengthen the semantic connection by identifying a word and its dependent words, while the dependency relationship between the head and the dependent can solve polysemy.

A larger number of experiments on natural language processing tasks show that SDE representations perform extremely well in practice. We can easily integrate SDE representations into the existing model, and achieve excellent indicators on six data sets of sentiment classification task and subject classification task.

2. Related work

Because of the ability to capture some syntactic and semantic information, pre-trained word vectors in [1] and [2] play an important role in many natural language processing tasks, such as question answering task in [13], textual entailment in [14] and the semantic role labeling in [15]. However, these word vectors have only a small amount of semantic information captured from the context within the window. In addition, since all words are mapped to a same vector space, the same word can only express one meaning in different contexts.

Some existing works try to overcome the above shortcomings by using different methods. For example, [5] and [6] extracted more sub-word features to enrich the word vector of the target word. Their methods benefit from sub-word units through the use of character convolutions. [7] used a novel method to learn the separate vector for each word. In recent years, more and more word was focused on

how to integrate the context features into the word vectors to get context-dependent representations. For example, [8] used bidirectional Long Short-term Memory (LSTM) to extract the information before and after the pivot word, and encoded the information into the pivot word to enrich the word representation. [16] used a supervised neural machine translation system and [17] used an unsupervised language model to learn contextual embedding. [10] has also address the problem of semantic similarity of different words in the same position by obtaining emotion-enriched word representations. [18] used a self-organizing map to get sentiment-based information. In our work, we also make full use of context-dependent information by semantic dependency parser in [3], which is based on Long Short-term Memory (LSTM).

3. SDE:Semantic Dependency Embedding

Unlike most widely used word embedding, Semantic Dependency Embedding is a more accurate word vector representation by fusing more semantic and syntactic information from semantic dependency analysis (Sec.3.3). Semantic Dependency Embedding consists of two parts,one is the word embedding obtained by traditional methods in [1] (Sec.3.1), and the other is the result obtained by semantic dependency parser (Sec.3.2).

3.1. Traditional word representation

The First architecture is Continuous Bag-of-Words Model[1]. The reason why CBOW model can achieve good results is that it uses the first few words and the last few words of the target word to predict the occurrence probability of the target word.

The model architecture is shown at fig. 1. In the input layer, each word is represented as a vector with dimension V after one-hot encoding operation, and V represents the total vocabulary. If the context has N words, the input dimension is $\mathrm{N}\times\mathrm{V}$. In the hidden layer, the input vector is projected into a new vector space using a matrix of dimension size $\mathrm{V}\times\mathrm{D}$. D is the word vector dimension we choose. In the output layer, the input vectors are summed and averaged, and then mapped by a matrix of dimension size $\mathrm{D}\times V$. Finally, a vector with dimension of $1\times\mathrm{V}$ is obtained after a softmax layer. The i-th value in the vector represents the probability that the target word is the i-th word in the dictionary.

The second architecture is Continuous Skip-gram Model [1]. Skip-gram model is similar to CBOW model, except that skip-gram model uses headwords to predict the occurrence probability of context words. After one-hot coding of the head word, the vector is mapped into the new vector space by a matrix with dimension $\mathrm{V}\times D$, and the probability of context word is obtained by using softmax layer after transformed by the matrix with dimension $\mathrm{D}\times V$. The model architectures is shown at fig. 2.

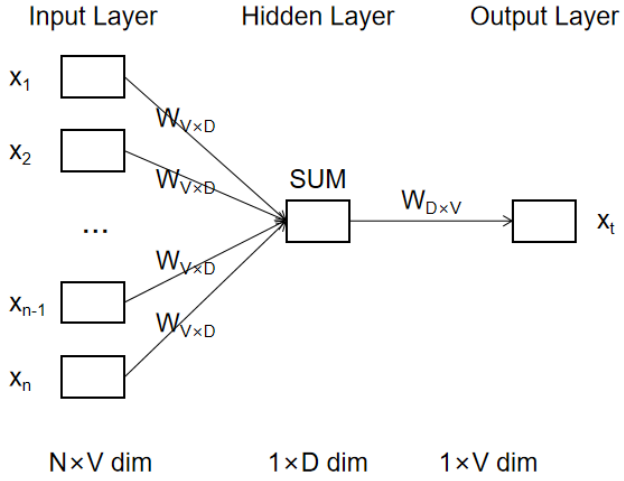


Fig.1 The CBOW model.

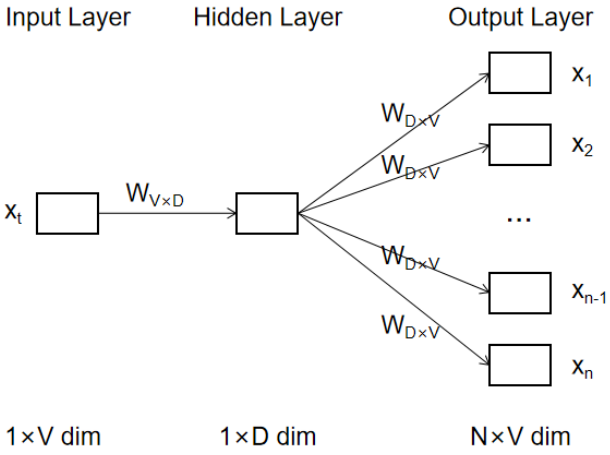


Fig.2 The Skip-gram model.

3.2. Semantic Dependency Parser

Semantic dependency parser aims at expressing a sentence as many pairs of related words and the dependency between each pair. The dependent (the first word in a word pair) and the head (the second word in a word pair) can enrich semantic information and strengthen the semantic connection by identifying a word and its dependent words, while the dependency relationship between the head and the dependent can solve polysemy.

For a sentence $\mathrm{S}=<w_1, w_2, ..., w_n>$, Semantic Dependency Parser will list all possible word pairs and

predict the possible dependency labels for each word pair. For example, the parser will split S into word pairs $< w_1, w_1 >$, $< w_1, w_2 >$, $< w_1, w_n >$,... , $< w_n, w_n >$. Then the parser will predicted the dependency labels of these word pairs. For cases like $<w_i, w_i>$, there is no dependency between the two words in this pair. We use this type of word pair to predict the root of a sentence.

The structure of the parser is shown in Fig. 3. The whole structure is composed of two layers, the lower layer is composed of bidirectional LSTM, and the upper layer is composed of a LSTM and an output layer.

In the lower layer, the input to the bidirectional LSTM is a sequence of n time steps, each representing a word in the sentence. In the training process, a hidden state is generated for each time step from the forward and backward directions at the same time. Then, we can get a forward hidden state and a backward hidden state. The two states are concatenated to form a hidden state as the output, which contains forward information and backward information. For one of the time steps x_t in a time series $X =< x_1, x_2, ..., x_n >$, after the processing of low layer, there are two hidden layers states: forward hidden state h_t and backward hidden state h_t', which are concatenated together as the output of this layer.

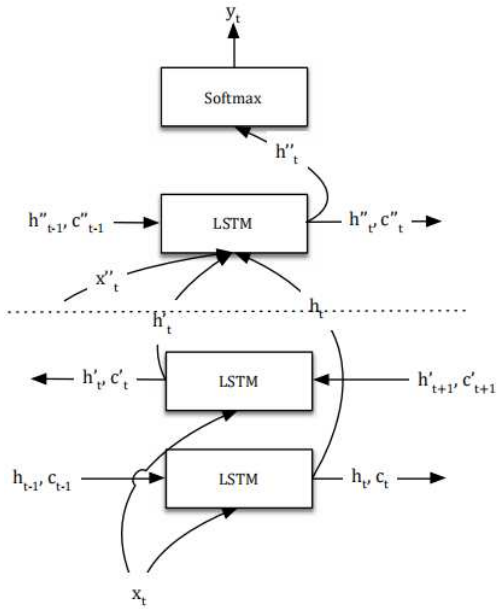


Fig.3 Sentiment Dependency Parser.

In the upper layer, the LSTM has two inputs, one is the feature representation (h_t, h_t') obtained from the lower layer, and the other is the input x_t''. After these two inputs pass through LSTM, we get a hidden state h_t'', which will be converted into the probability distribution of labels after passing through softmax layer. fig. 4 illustrates an example of semantic dependency graph. Here, "她(she)" is the head of "脸色(face)" and at the same time it is an head of "病(disease)". Meanwhile, the relationship between the two word pairs is different, one is "Poss" and the other is "Exp" . Using these information can make the word representation have more semantic dependency information to improve the effect of downstream tasks.

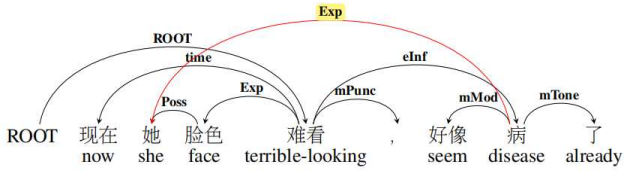


Fig.4 An example of semantic dependency representation.

3.3. Fusion For SDE

Through traditional word vector model in Sec.3.1, we can get the basic word vector. Using continuous distributed representation of the context, these basic word vector can record some simple semantic information by position. fig. 5 shows us how we get the basic word vector, where E is the basic word vector.

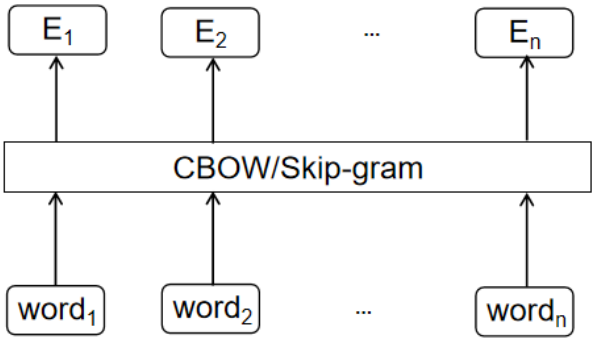


Fig.5 The process of obtaining basic CBOW/Skip-gram word vector.

When input is a sentence containing n words(e.g. $S= < w_1, w_2, ... , w_n >$), Semantic Dependency Parser will output n word pairs (e.g. $< w_1, w_x >$) and corresponding n relationships. We call the first word in the pair "dependent" and the second word "head". For each word, the header information and corresponding relationship information have rich semantic information, the head information indicates which word in the sentence the word depends on, and the relation information indicates which kind of dependency the two words belong to.

We use two weight matrices to encode head information

and relation information respectively, and the size of the weight matrix is $N \times D$, where N represents the total size of head or relation, and D is the dimension of the encoded vector. The header information can be obtained through a projection layer, which is the same as the one in the traditional word vector model. We construct the matrix of the relationship according to the sum of relationship from the Semantic Dependency Parser to encode the relationship information. This process is shown in fig. 6, where EH and ER represent the result vector of head information and relation information respectively.

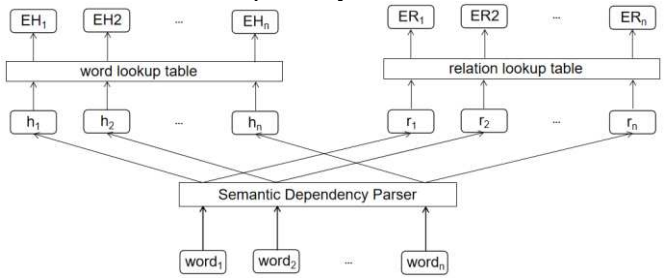


Fig.6 The process of using weight matrices to encode head information and relation information.

Finally, by fusing these vectors(e.g.E, EH, ER) we have obtained, Semantic Dependency Embedding(SDE) is formed, which can be divided into Semantic Dependency Embedding from CBOW(SDEC) and Semantic Dependency Embedding from Skip-gram(SDES) according to the basic word vector. SDEC has less training time than SDES, while SDES handles rare words better than SDEC. fig. 7 shows the integration process.

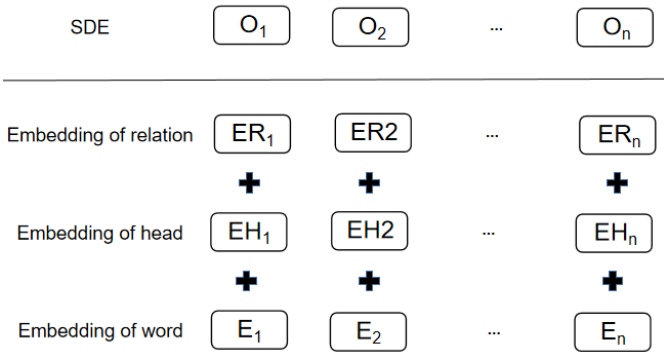


Fig.7 The formation process of SDE.

4. Experiments

In this section, we use SDE and apply it to sentiment classification and topic classification. The advantages of SDE are illustrated by a large number of experiments.

4.1. Datasets

We choose three public data sets for sentiment classification: Hotel Review Polarity (Hotel.P), Weibo Review Polarity (Weibo.P) and Takeaway Review Polarity (Takeaway.P), and three for topic classification: Goods Classification data set (Goods), News Classification data set (News) and News Title data set (News Title). Table 1 and Table 2 give more detailed information on these data sets.

Table 1 Features of sentiment classification data sets.

Data set	Positive	Negative	Total
Hotel.P	5,322	2,443	7,765
Weibo.P	59,993	59,995	119,998
Takeaway.P	4,000	7,987	11,987

Table 2 Features of subject classification data sets.

Data set	Categories	Total
Goods	5	5,000
News	15	150,000
News Title	13	130,000

4.2. Preprocessing and postprocessing

First,we use regular expressions to filter punctuation marks and stop words in the sentences. After filtering, sentences less than 5 in length are excluded. Then we use Semantic Dependency Parser(SDP) for word segmentation to get the word, the head of the word as well as their semantic relationship and consider words with less than three occurrences as OOV. The SDP model we use mentioned in Sec.3.2. During the training of the SDP model, we choose Negative Log-likelihood function as the loss function. The goal of training is to minimize the gap between the predicted dependency and the real dependency for each word pair. We use mini-batch update and Adagrad[12] to optimize the parameter learning. We will also pre-train the CBOW and Skip-gram models. In the training process, the window size is set to 5, min-count is set to 3, and the dimension of word vector is set to 128.

For down-stream tasks, we built a basic classification framework, which consists of a bidirectional LSTM layer and a fully connected layer. The bidirectional LSTM with a hidden size of 256 uses the preprocessed SDE as input. A hidden state is generated for each time step from the forward and backward directions at the same time. Then, we can get a forward hidden state and a backward hidden state. The two states are concatenated to form a hidden state as the output, which contains forward information and backward information. Finally, after passing through a full connection layer and softmax layer, we can get the predicted results.

4.3. Results

From table 3 and table 4,we can see that the accuracy of SDEC and SDES on the six data sets are higher than the word vectors based on the traditional CBOW and Skip-gram models. It can be seen from the table that the SDE based on CBOW(SDEC) performs well on sentiment classification tasks, while SDES performs better on topic classification tasks. In fig. 8-10, We choose several of these data sets to show the accuracy and loss of different word vectors in the training process. In the training process,we used the early-stop mechanism and ensured that the parameters of the model were determined by the iteration with the smallest loss. Obviously, the word representation proposed in this paper has achieved state-of-art in these six public data sets, which performs well than the word representations based on CBOW and Skip-gram.

Table 3 Accuracy of sentiment classification data sets.

Model	Hotel.P	Weibo.P	Takeaway.P
CBOW	0.83	0.69	0.87
Skip-gram	0.67	0.68	0.85
SDEC	**0.86**	**0.72**	**0.9**
SDES	0.7	**0.72**	0.89

Table 4 Accuracy of subject classification data sets.

Model	Goods	News	News Title
CBOW	0.89	0.82	0.83
Skip-gram	0.89	0.81	0.84
SDEC	0.88	**0.84**	0.83
SDES	**0.89**	0.82	**0.84**

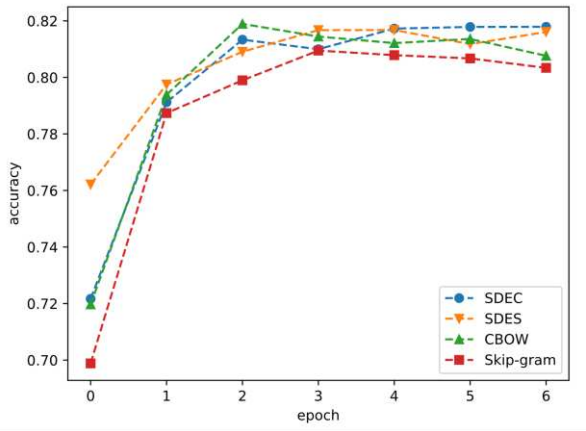


Fig.8 Accuracy on News data set.

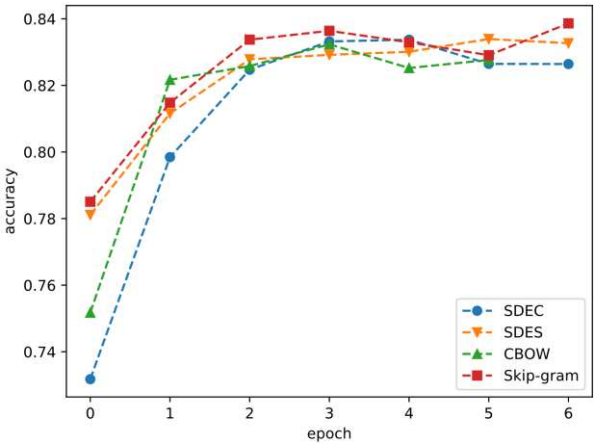


Fig.9 Accuracy on News Title data set.

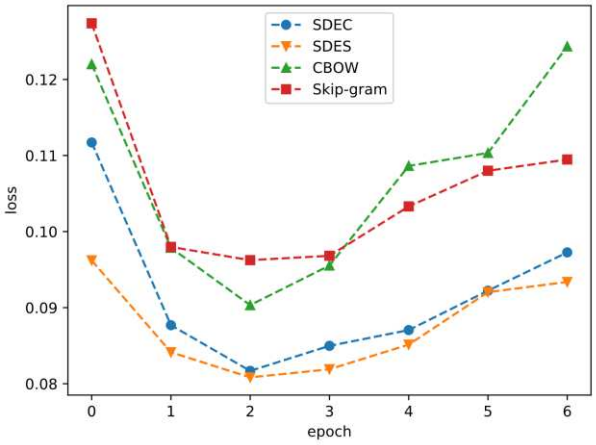


Fig.10 Loss on News data set.

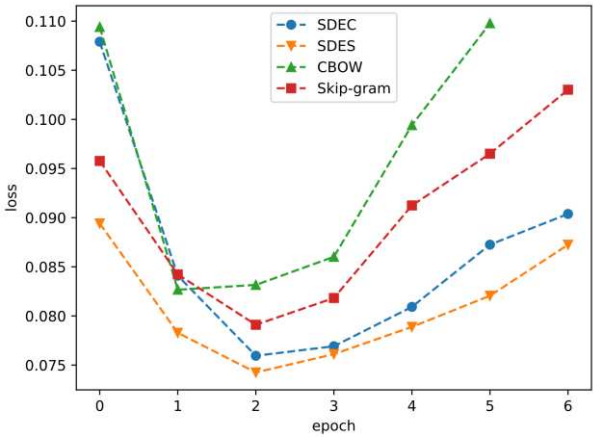


Fig.11 Loss on New Title data set.

5. Conclusions

We have introduced a general approach for learning high-quality word representation by fusing semantic dependency information,which solves problems well and show improvements when applying SDE to sentiment classification task and topic classification task. Through a large number of experiments, the performance of this method is compared with that of CBOW and Skip-gram model. It shows SDE contains rich semantic dependency information,which can better express the meaning of a sentence. In the future, SDE can be used as a pre-training word representation to serve more NLP tasks to improve the quality of tasks.

Acknowledgements

The study is supported by Core Curriculum Platform Construction Project in Computer Network, School of Information and Software Engineering, University of Electronic Science and Technology of China.

References

[1] Mikolov T . Distributed Representations of Words and Phrases and their Compositionality[J]. Advances in Neural Information Processing Systems, 2013, 26:3111-3119.

[2] Pennington J , Socher R , Manning C . Glove: Global Vectors for Word Representation[C]// Conference on Empirical Methods in Natural Language Processing. 2014.

[3] Jin L , Duan M , Schuler W . OCLSP at SemEval-2016 Task 9: Multilayered LSTM as a Neural Semantic Dependency Parser[C]// Proceedings of the 10th International Workshop on Semantic Evaluation (SemEval-2016). 2016.

[4] Turian J P , Ratinov L A , Bengio Y . Word representations: A simple and general method for semi-supervised learning[C]// Acl, Meeting of the Association for Computational Linguistics, July, Uppsala, Sweden. DBLP, 2010.

[5] Wieting J , Bansal M , Gimpel K , et al. Charagram: Embedding Words and Sentences via Character n-grams[J]. 2016.

[6] Bojanowski P , Grave E , Joulin A , et al. Enriching Word Vectors with Subword Information[J]. Transactions of the Association for Computational Linguistics, 2017, 5:135-146.

[7] Neelakantan A , Shankar J , Passos A , et al. Efficient Non-parametric Estimation of Multiple Embeddings per Word in Vector Space[J]. Computer ence, 2015.

[8] Melamud O , Goldberger J , Dagan I . context2vec: Learning Generic Context Embedding with Bidirectional LSTM[C]// Proceedings of The 20th SIGNLL Conference on Computational Natural Language Learning. 2016.

[9] Hochreiter S , Schmidhuber J . Long Short-Term Memory[J]. Neural Computation, 1997, 9(8):1735-1780.

[10] Agrawal A, An A, Papagelis M, et al. Learning Emotion-enriched Word Representations[C]. international conference on computational linguistics, 2018: 950-961.

[11] Y. Bengio, R. Ducharme, P. Vincent. A neural probabilistic language model. Journal of Machine Learning Research, 3:1137-1155, 2003.

[12] Duchi. J. and Hazan. E., Adaptive subgradient methods for online learning and stochastic optimization, Journal of Machine Learning Research, pp. 2121-2159, Jul. 2011.

[13] Xiaodong Liu, Yelong Shen, Kevin Duh, et al. Stochastic Answer Networks for Machine Reading Comprehension[J]. 2018.

[14] Chen Q , Zhu X , Ling Z , et al. Enhanced LSTM for Natural Language Inference[J]. 2016.

[15] He L , Lee K , Lewis M , et al. Deep Semantic Role Labeling: What Works and What's Next[C]// Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers). 2017.

[16] Mccann B , Bradbury J , Xiong C , et al. Learned in Translation: Contextualized Word Vectors[J]. 2017.

[17] Peters M E, Ammar W, Bhagavatula C, et al. Semi-supervised sequence tagging with bidirectional language models[J]. arXiv preprint arXiv:1705.00108, 2017.

[18] Sagnika Santwana,Mishra Bhabani Shankar Prasad, Meher Saroj K.. Improved method of word embedding for efficient analysis of human sentiments[J]. Multimedia Tools and Applications,2020,79(43-44).

3DCNN: THREE-LAYERS DEEP CONVOLUTIONAL NEURAL NETWORK ARCHITECTURE FOR BREAST CANCER DETECTION USING CLINICAL IMAGE DATA

AMIN UL HAQ[1], JIAN PING LI[1], ABDUS SABOOR[1], JALALUDDIN KHAN[1], WANG ZHOU[2], TAO JIANG[1], MORDECAI F. RAJI[1], SAMAD WALI[3]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[2]School of Computer and Software Engineering, Xihua University, Chengdu 610039, P.R. China
[3]Department of Mathematics, Namal Institute, Talagang Road, Mianwali 42250, Pakistan
E-MAIL: khan.amin50@yahoo.com, jpl2222@uestc.edu.cn, sabbor_khan97@yahoo.com, alal4amu@yahoo.com, dean_uestc@163.com, tao1024@yahoo.com, mraji@qq.com.

Abstract:

The breast cancer is a critical female disease and its proper identification is very essential for better cure and recovery. The diagnosis of BC is a critical issue for clinical specialists and scholars. Different researchers proposed breast cancer diagnosis methods using deep learning techniques. However, these proposed methods not diagnosis breast cancer accurately. In order to tackle the issue of accurate detection of breast cancer we proposed a 3-layers CNN architecture for accurate detection of breast cancer. The proposed model has been trained and tested on Breast histology images data set. The cross validation method Hold out has been applied for best model selection and hyper parameters tuning. Furthermore, different model evaluation metrics have been used for model performance evaluation. The experimental results demonstrated that propped method is more suitable for breast cancer and it would be incorporated in health care successfully.

Keywords:

Breast cancer; Classification; Deep Learning; Convolutional neural network; Image data set; Prediction accuracy

1. Introduction

Breast Cancer (BC) is one the most chronical disease of women in the world and women death 5th major reason is breast cancer comparatively to other kinds of cancers [1, 21]. A group of splitting cells inside the breast tissues are develops which is called Tumors and these tumors can be cancerous non-cancerous. To diagnosis breast cancer numerous invoice based techniques have been used for detection of BC. Biopsy [2] method breast tissues use for diagnosis and obtained results are highly accurate. While mammogram [3] method of detection of breast cancer 2Dimensionals projection image is created from breast. Another invasive based method Magnetic Reasoning imaging (MRI) [4] has been used for BC detection. However, invoice based techniques for breast cancer diagnosis are not accurately and efficiently detect BC.

These issues of invasive based BC diagnosis can be effectively address by non-invasive based methods such as machine learning and deep learning. Specifically, deep learning models such as Convolutional neural network (CNN) [5] are mostly used for detection of breast cancer and the performance of CNN in clinical imaging is very high [6]. CNNs model from training image dataset automatically learn and selects more relevant features for classification [7]. In literature mostly lately Xu et al. [8] used U-NET CNN architecture for detection of BC. Leyy at al. [9] employed CNN, AlexNet, GoogleNet for breast cancer detection using ImageNet dataset. Rasti et al. [10] designed a CNN Model based mixture ensemble for classification of benign and malignant.

In this research study main aim to classify cancerous images (IDC: invasive ductal carcinoma) vs non-IDC images using CNN model. The CCN model has very high performance in classification of image medical data and extract relevant features from image automatically. Breast histology images data set has been used for training and testing of the proposed model. Cross validation method Hold out has been employed for model validation. Additionally, performance evaluation metrics have been used for CNN performance evaluation.

The rest sections of the paper organized as: In section 2 Breast histology images data set and proposed 3- layer CNNs model have been described in details. Section 3 is experimental work section in we performed different

experiments and discussed experimental results. The section 4 in conclusion and future work

2. Materials and methods

2.1. Data set

Invasive Ductal Carcinoma (IDC) is the most common subtype of all breast cancers. In order to classify cancerous IDC and non-cancerous IDC images, we used Breast histology images data set which available on kaggle Machine learning repository [11]. This dataset consists of 5547 breast histology images of size 50 x 50 x 3, curated from Andrew Janowczyk website and used for a data science tutorial at Epidemium. The goal is to classify cancerous images (IDC: invasive ductal carcinoma) vs non-IDC images. In fig. 1 the data set is given.

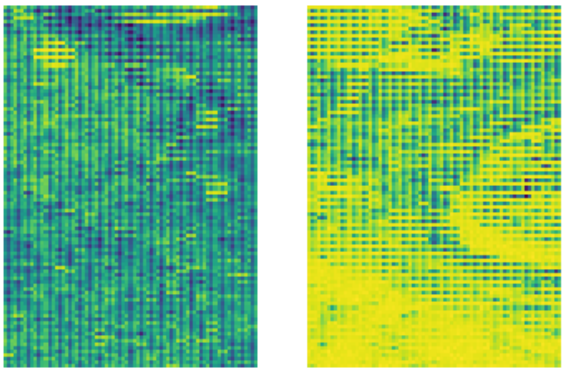


Fig.1 Breast histology images data set

2.2. Deep learning model

In this research work deep learning model (CNN) for Breast cancer detection has been employed. Deep Learning is a kind of Algorithm of Machine Learning which integrate Feature Selection, and Classification process for better performance [12, 13, 14, 15]. Extraction of feature from Input Data are incorporate to build CNN Model and evaluating model performance on testing phase. CNN is deep learning model which have neurons, weights, loss function and other parameters. In architecture of CNN have layers of three types, such as Convolutional layer, pooling layer, and lastly fully linked layer [16, 17]. The input data to CNN convolved by convolutional layer and map into features, then these feature passed from pooling layer which prevents overfitting by dropping parameters and computation in Network Structure. Finally, the fully Connected Layer is used for grouping. Furthermore, learning rate is parameter which defined the model learning process through training. CNN also use some activation function such as ReLU, tanh and softmax for layers' activation. Different optimizers have been used for optimization purpose such as stochastic gradient descent, Adam, Adadelta, RMSprop in CNN model. The generic CNN model is given in fig. 2.

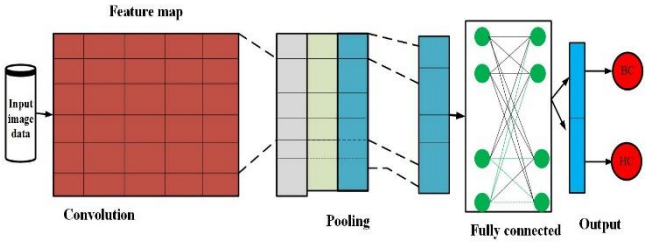


Fig.2 Generic CNN model for breast cancer detection

2.3. Proposed Deep Convolution Neural Network Model

We proposed a DnCNN model for classification of cancerous IDC and non-cancerous IDC images. In development of the CNN model three layers have been used in which one is input layer and use for inputting image data, three layers are hidden which are used for internal transformation, and last layer is fully connected output layer which has been used to classify cancerous IDC and non-cancerous IDC images. The input image data has been used for training and evaluation of the model. In the proposed DnCNN model hold out cross validation method has been used for model training and validation. Activation function such as ReLU has been used for all layers, and softmax for output layer has been used. We used different optimizer Adam in our model [12, 18, 19] with different learning rates. The dropout has been adjusted 0.5. For model performance evaluation, various evaluation metrics have been used such as accuracy, sensitivity, specificity, F1-score, MCC, and AUC.

The inputs of model of shape 50×50×3 Image used at the first Convolutional Layer along 32 kernels of shape 32×7×7×1 and stride of pixel 1. The Convolutional Layer second inputs the layer 1 output with 64 kernels of shape 5×5×32. The third layer has 128 kernels of shape 3×3×64 to output layer connected. Max-pooling, batch normalization layers are interconnected with each convolutional layer. With last layer dropout layer applied before to stop overfitting of DnCNN model.

The other important parameters of different layers of DnCNN model have been reported in Table 1.

Table 1 DnCNN model parameters and layers description

No of layer	Layer name	structure	Activation	parameters	Number of parameters
1	Input image	50×50×3	50×50×3	-	0
2	2D Convolution	32×7×7×1convolution with [1 1] Stride &[1 1 1] Padding	46×64×32	7×7×1×32 weights 1×1×32 bias	1600
3	Batch normalization	32 filters	46×64×32	1×1×32 offset 1×1×32 scale	64
4	Activation function	Re-LU	46×64×32	-	0
5	2D-Max-pooling	2×2 Pooling [2 2] Stride & [1 1 1] Padding	23×2346×64×3264	-	-
6	2D convolution	64×5×32 Convolution with[1 1] Stride & [1 1 1] Padding	21×21×64	5×5×32×64 weights 1×1×64 bias	51264
7	Batch normalization	64 filters	21×21×64	1×1×64 offset 1×1×64 scale	128
8	Activation function	Re-LU	21×21×64	-	0
9	2D-Max-Pooling	2×2 pooling [2 2] stride & [0 0 0] padding	10×10×64	-	0
10	2D convolution	128×3×3×64 convolution [1 1] stride & [1 1 1 1]	1×1×128	3×3×64×128 weights 1×1×128	9437184
11	Batch normalization	128 filters	1×1×128	1×1×128 offset 1×1×128 scale	16384
12	Activation function	ReLU	1×1×128	-	0
13	Dropout	0.5%	1×1×128	-	0
14	Fully connected layer	2	1×1×2	2×128 weights 2×1 bias	16384
15	Activation function output	Softmax	1×1×2	-	0
16	output	cancerous IDC and non-cancerous IDC images.	-	-	9523008

2.4. DnCNN model cross validation mechanism

To train and test our model DnCNN we have been used Hold [26, 27, 28, 29] out cross validation method. The image data set splits into two parts 80% for training and 20% for testing of the model.

2.5. DnCNN model performance evaluation criteria

The proposed model DnCNN performance has been evaluated by employing various performance evaluation metrics such as accuracy, specificity, sensitivity, MCC, precision, F1-score, AUC and model processing time [20, 21, 22, 23, 24,25]. Mathematically these metrics have been written in equations (1), (2), (3), (4) and (5) respectively.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \text{x}100\% \quad (1)$$

$$\text{Sensitivity} = \frac{TP}{TP+FN} \text{ x}100\% \quad (2)$$

$$\text{Specificity} = \frac{TN}{TN+FP} \text{ x}100\% \quad (3)$$

$$\text{Precision} = \frac{Tp}{Tp+FP} \text{ x}100\% \quad (4)$$

$$\text{MCC} = \frac{TP\times TN-FP\times FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \text{ x}100\% \quad (5)$$

2.6. Proposed DnCNN model Procedure

The Pseudo-code of the proposed DnCNN model is given in Algorithm1.

Alg.1 Pseudo-code of proposed DnCNN model for Breast cancer diagnosis

Step1: Begin
Step2: Pre-processing of Breast histology images data set;
Step3: Trained DnCNN on training data set with different parameters;
Step4: Validated DnCNN on testing data set;
Step5: Computes DnCNN performance;
Step6: End

3. Experimental results analysis and discussion

The DnCNN model has been trained and validated on Breast histology images data set. The hold out cross validation method has been employed with 80% and 20% for training and validation respectively. The others parameters need for DnCNN have been reported in Table 2. The model

performance evaluation metrics such as accuracy, specificity, sensitivity, MCC, precision, F1-score and processing have been computed and reported in Table 3. The DnCNN model has been developed in programming language python using keras and running on computer system with configuration of Intel Core TM i5-2410M, 4GB random access memory with 640BG hard drive, window 10.

According to Table 3, the proposed DnCNN model obtained 79 % accuracy, 98% specificity, 96% sensitivity, 97% MCC, 85% precision, F1-score 82% and AUC value was 85%. The model computation time was 30 minutes respectively. The training loss and validation loss and training accuracy and validation accuracy of the DnCNN model has been shown in fig. 3 for better understanding the model performance. The experimental results demonstrated that proposed model performance is high and its recommended for diagnosis of breast cancer.

Table 2 DnCNN model others parameters

No of maximum epochs	Learning rate	Training part of data set	Testing part	Optimizer	Batch size	Dropout	Output activation function	Inner activation function of layers
60	0.0001	(4437)80%	(1109)20%	Adam	128	0.5	Softmax	ReLU

Table 3 DnCNN model performance evaluation results

Acc(%)	Sp(%)	Sn(%)	MCC(%)	Pre(%)	F1score(%)	AUC(%)	Time(m)
79	98	96	97	85	82	85	30

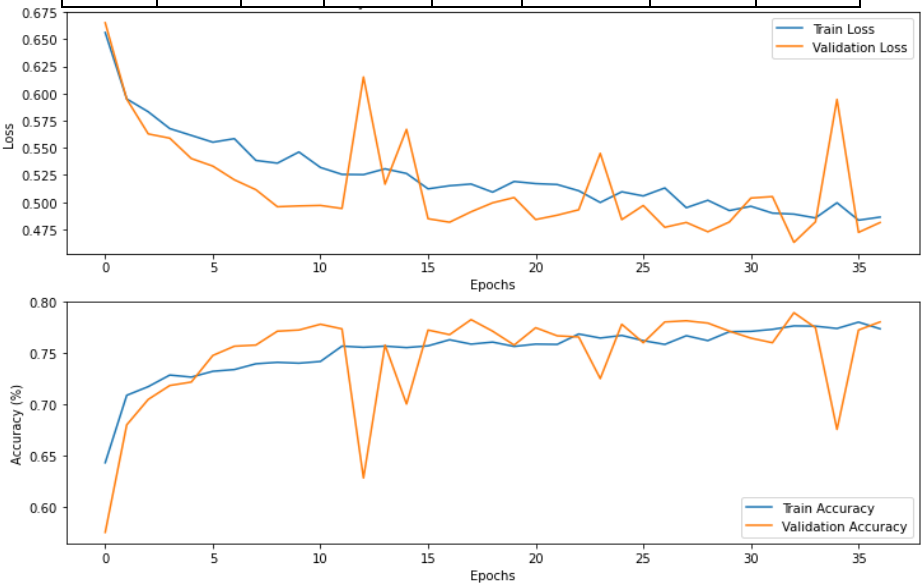


Fig.3 Accuracy and loss of the proposed model

4. Conclusions

The deep learning convolution neural network (DnCNN) model is more suitable for medical image data processing. To diagnosis breast cancer through breast image data we proposed DnCNN model and the proposed model obtained very high performance in terms of accuracy. The accuracy has been obtained 79% and computation time of model was 30 minutes. Due to excellent performance of DnCNN model we recommend it for diagnosis of breast cancer. In future work we will performance more experiments with others deep learning models for diagnosis of breast cancer using breast cancer images data sets.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, the project of Science and Technology Department of Chongqing Municipality, Chengdu Chengdian Network Technology Co., Ltd., Chengdu Civil-military Integration Project Management Co., Ltd., and Sichuan Yin Ten Gu

Technology Co., Ltd.

References

[1] American institute for breast cancer research., https://www.wcrf.org/dietandcancer/ cancer-trends/breast-cancer-statistics. Accessed: 2020-10-13.

[2] A. M. Ahmad, G. M. Khan, S. A. Mahmud, and J. F. Miller,"Breast cancer detection using cartesian genetic programming evolved artificial neural networks," in Proceedings of the 14th Annual Conference on Genetic and Evolutionary Computation, GECCO '12, (New York, NY, USA), pp. 1031–1038, ACM,2012.

[3] A. T. Azar and S. A. El-Said, "Probabilistic neural network for breast cancer classification," Neural Computing and Applications, vol. 23, no. 6, pp. 1737–1751, 2013.

[4] E. Warner, H. Messersmith, P. Causer, A. Eisen, R. Shumak,and D. Plewes, "Systematic review: using magnetic resonance imaging to screen women at high risk for breast cancer," Annals of internal medicine, vol. 148, no. 9, pp. 671–679, 2008.

[5] LeCun Y, Bottou L, Bengio Y, Haffner P (1998) Gradient-based learning applied to documentrecognition. Proc IEEE 86(11):2278–2324

[6] Havaei M, Davy A, Warde-Farley D, Biard A, Courville A, Bengio Y, Pal C, Jodoin PM, Larochelle H (2017) Brain tumor segmentation with deep neural networks. Med Image Anal 35:18–31

[7] Hoo-Chang S, Roth HR, Gao M, Lu L, Xu Z, Nogues I, Yao J, Mollura D, Summers RM (2016) Deep convolutional neural networks for computer-aided detection: Cnn architectures, dataset characteristics and transfer learning. IEEE Trans Med Imaging 35(5):1285.

[8] Xu X, Fu L, Chen Y, Larsson R, Zhang D, Suo S, Hua J, Zhao J (2018) Breast region segmentation being convolutional neural network in dynamic contrast enhanced mri. In: 2018 40Th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), IEEE, pp 750–753.

[9] L´evy D, Jain A (2016) Breast mass classification from mammograms using deep convolutional neural networks. arXiv:1612.00542

[10] Rasti R, Teshnehlab M, Phung SL (2017) Breast cancer diagnosis in dce-mri using mixture ensemble of convolutional neural networks. Pattern Recogn 72:381–390.

[11] Breast histology images data set on kaggle machine learning repository, https://www.kaggle.com/simjeg/lymphoma-subtype-classification-fl-vs-cll, Accessed on 10 October 2020.

[12] Oh, Shu Lih, et al. "A deep learning approach for Parkinson's disease diagnosis from EEG signals." Neural Computing and Applications (2018): 1-7.

[13] Acharya UR, Fujita H, Oh SL, Hagiwara Y, Tan JH, Muhammad A (2017) Automated detection of arrhythmias using different intervals of tachycardia ECG segments with convolutional neural network. Inf Sci 405:81–90

[14] Acharya UR, Fujita H, Oh SL, Muhammad A, Tan JH, Chua KC (2017) Automated detection of coronary artery disease using different durations of ECG segments with convolutional neural network. Knowl Based Syst 132:62–71

[15] Acharya UR, Fujita H, Oh SL, Hagiwara Y, Tan JH, Muhammad A, Tan RS (2018) Deep convolutional neural network for the automated diagnosis of congestive heart failure using ECG signals. Appl Intell 13:1–12

[16] Acharya UR, Fujita H, Oh SL, Raghavendra U, Tan JH, Muhammad A, Gerytch A, Hagiwara Y (2018) Automated identification of shockable and non-shockable life-threatening ventricular arrhythmias using convolutional neural network. Future Gener Comput Syst 79(3):952–959.

[17] Faust O, Hagiwara Y, Tan JH, Oh SL, Acharya UR (2018) Deep learning for healthcare applications based on physiological signals: a review. Comput Methods Prog Biomed 161:1–13]

[18] Khatamino, Pedram, İsmail Cantürk, and Lale Özyılmaz. "A Deep Learning-CNN Based System for Medical Diagnosis: An Application on Parkinson's Disease Handwriting Drawings." 2018 6th International Conference on Control Engineering & Information Technology (CEIT). IEEE, 2018.

[19] L´evy D, Jain A (2016) Breast mass classification from mammograms using deep convolutional neural networks. arXiv:1612.00542.

[20] Haq, Amin Ul, et al. "Intelligent Machine Learning Approach for Effective Recognition of Diabetes in E-Healthcare Using Clinical Data." Sensors 20.9 (2020): 2649.

[21] Ul Haq, Amin, et al. "A novel integrated diagnosis method for breast cancer detection." Journal of Intelligent & Fuzzy Systems Preprint (2020): 1-16.

[22] Haq, Amin Ul, et al. "Feature selection based on L1-norm support vector machine and effective recognition system for Parkinson's disease using voice recordings." IEEE access 7 (2019): 37718-37734.

[23] Haq, Amin Ul, et al. "Comparative analysis of the classification performance of machine learning classifiers and deep neural network classifier for prediction of Parkinson disease." 2018 15th

International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP). IEEE, 2018.
[24] HAQ, AMIN UL, et al. "Identifying the Predictive Capability of Machine Learning Classifiers for Designing Heart Disease Detection System." 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing. IEEE, 2019.
[25] HAQ, AMIN UL, et al. "Identifying the Predictive Capability of Machine Learning Classifiers for Designing Heart Disease Detection System." 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing. IEEE, 2019.
[26] Haq, Amin Ul, et al. "A hybrid intelligent system framework for the prediction of heart disease using machine learning algorithms." Mobile Information Systems 2018 (2018).
[27] Li, Jian Ping, et al. "Heart Disease Identification Method Using Machine Learning Classification in E-Healthcare." IEEE Access 8 (2020): 107562-107582.
[28] Haq, Amin Ul, et al. "Heart Disease Prediction System Using Model of Machine Learning and Sequential Backward Selection Algorithm for Features Selection." 2019 IEEE 5th International Conference for Convergence in Technology (I2CT). IEEE, 2019.
[29] Ul Haq, Amin, et al. "Recognition of the parkinson's disease using a hybrid feature selection approach." Journal of Intelligent & Fuzzy Systems Preprint: 1-21.

EFFECT OF MAHA MRITYUNJAYA HYMN RECITATION ON HUMAN BRAIN FOR THE ANALYSIS OF SINGLE EEG CHANNEL C4-A1 USING MACHINE LEARNING CLASSIFIERS ON YOGA PRACTITIONER

RISHIPAL[1], MD BELAL BIN HEYAT[2], ZILI YOU[1*], BALARAM PARDHAN[3], FAIJAN AKHTAR[4], SYED JAFAR ABBAS[5], BISHAL GURAGAI[1], KADAMBINI ACHARYA[3]

[1]School of Life Science and Technology, University of Electronic Science and Technology of China, Chengdu, 610054, China

[2]Biomedical Imaging and Electrophysiology Laboratory, School of Electronic Science and Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan, 610054, China

[3]Department of Yoga and Humanities, Swami Vivekananda Yoga Anuasandhana Samsthana, Yoga University, Bangalore, Karnataka, 560 102, India

[4]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan, 611731, China

[5]School of Automation Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan, 611731, China

E-MAIL: youzili@uestc.edu.cn

Abstract:

Maha mrityunjaya hymn is Hindu religious belief to control the mind to dedicate Lord Shiva. Many seers have been practicing it since ancient time. The main aim of this paper is to find the changes in brain signal using C4-A1 channel of the Electroencephalogram (EEG) signal during recitation of this hymn. This study was completed in some steps such as real time EEG recording, extraction of the C4-A1 channel, preprocessing, calculation of the power spectral density, and classification using Decision Tree (DT) and K-Nearest Neighbor (KNN) on five yoga practitioners. The KNN classifier having 5-fold cross validation model achieved the highest recall (97.4%) and accuracy (97.4%) of the system. We obtained that the average frequency of the EEG wave increased prominently. This study will be helpful for the people to understand in the scientific way for the recitation of the religious hymn.

Keywords:

Brain; Maha mrityunjaya hymn; Hinduism; Decision tree; KNN; EEG; Yoga

1. Introduction

The ultimate goal of life is to achieve the original state or self-realization for every human. The great saints around the world had recognized this. Most of them had used the path of surrender to their master (almighty Lord/Gods) based of their cultures or the religions. They have communicated to the master through their prayer prescribed in their religious text. Most often they pray for duration regularly everyday by repetition of a syllable or a sentence. This exercise over a time period helps them to achieve a state of meditation. In general it brings a state of mindfulness, developed concentration, and provides alter-full relaxation. The beneficial effect of meditation had been well documented in scientific literature that meditator found to gain better psychological health and good control over emotions.

In specific to the Muslim prayer found to be enhancing relaxation by reducing the anxiety by increasing the parasympathetic activity during Salat prayer [1]. Further, while reciting prayer during Salat practice the mean gamma activity increased significantly in comparison to the mimic Salat practice. This is an indication of enhancing the cognitive and attention process which may lead to focus attention meditation mood [2]. It was also observed that alpha activity saw higher values while performing prostration position in Dhuha prayer at a partial and occipital area in comparison to the resting condition [3]. In transcendental meditation practitioner used a hymn provided by his spiritual master repetition of this hymn as a part of this meditation which pushes the practitioner to a state of a higher plane of consciousness. Scientific indications were documented by observing in decrease in oxygen consumption, breath rate and heart rate, and blood lactate levels while increase in alpha and theta activity of EEG signal [4], [5]. This was an indication of autonomic stability and a feeling of calming state of mind [6].

Neurohemodynamic deactivation was documented during the chanting of "*OM"* in different brain regions while no changes occur by mimic *"SSSS"* pronouncing in comparisons to the resting state. This is an indication of limbic deactivation suggested that clinical application of psychiatric patients [7]. Further in an fMRI study showed a deactivation of brain regions during *"OM"* chanting [8]**.** In another study of *"OM"* hymn meditation found that higher theta amplitude after meditation at all regions in comparison to the before meditation [9].

In the proposed work, we used C4-A1 channel of the EEG signal to find the effect of *"maha mrityunjaya hymn"* recitation in human brain. We used the Blackman window having a finite impulse response filter for the preprocessing of the signal. After preprocessing, we used the welch method for the extraction of the Power Spectral Density (PSD) of the signal as a feature. Finally, we applied the DT and KNN classifier for the performance of the proposed system.

2. Proposed Dataset

In total, five male yoga practitioner without any heart and mental disease recruited from a Swami Vivekananda Yoga Anuasandhana Samsthana, Yoga University, Bangalore in India. Their ages range from 18 to 22 and health were checked by the public hospital. The participants were gave their written consent for the study. The study was approved through the ethical committee of the university. We used sleep polysomnography for the recording of the EEG signal on the yoga practitioner. The data collected phase is divided into three parts: 1) 5 minutes of pre-condition, 2) 10 minutes of *maha mrityunjaya hymn* recitation, and 3) 5 minutes of silently sat. In this work, we extracted single C4-A1 channel of the EEG signal to analyze the data.

3. Methods

3.1. Calculation of Power Spectral Density (PSD)

We estimated the PSD using the Welch method, it is introduced in 1967. It converts time series into segment data, calculating a modified periodogram of every segment, and take the average of power spectral density. The average altered periodogram tends to reduce the variance. As well, estimate the relation to a single periodogram of aggregate data. While overlay among segments introduces irrelevant facts, this result is reduced using a non-rectangular window, which decreases weight given to the end samples of the segment [10-16]. The Welch techniques are described in equations (1), (2), and (3) below:

$$U = \frac{1}{L}\sum_{n=0}^{L-1}\left[w(n)\right]^2 \tag{1}$$

$$P = \frac{1}{LU}\sum_{n=0}^{L-1}\left[w(n)\,x(n+iD)\,e^{-j2\pi fn}\right]^2 \tag{2}$$

$$P = \gamma\sum_{i=0}^{L-1}\left[\left(X_a^i\right)^2 + \left(X_b^i\right)^2\right] \tag{3}$$

Where U is equal to compensate for the loss of signal, L and D is the data of the segment, $w(n)$ is the hamming window, X_a^i & X_b^i are the real and imaginary part of the i^{th} segment, and P is the Welch method.

3.2. 3.2. Decision Tree (DT) classifier

DT is a simple demonstration for categorizing problems. It is one of the supervised machine-learning algorithms, where data are continuously dividing based on certain parameters. It consists of edges or branches, nodes, and leaf nodes [17]. It is divided into two parts such as classification tree and regression tree [16]. We used classification tree in this work. Our parameters of this classifier are two minimum numbers of instances in leaves, the split subset must be smaller than five must, and maximal limit of the tree depth is one hundred. The advantages of the DT classifier are inexpensive, fast, excluded noises, easy to interpret, and more accurate than other classifiers. DT is described in equation (4) and (5):

$$E(H_t) = \textstyle\sum_i P_i H_i \tag{4}$$

$$R_t = H - E(H_t) \tag{5}$$

Where, H_t is the average uncertainty after performing test t, P_i is the probability that the test has j outcome, and R_t is the average reduction in uncertainty achieved by test t.

3.3. K- Nearest Neighbor (KNN) classifier

KNN is a procedure that stores all accessible cases and classifies novel cases based on a distance function. KNN has been used in pattern recognition and statistical estimation in 1970. The case is categorized by a popular vote of its neighbors. KNN is used in both classification and regression analytical problems [18]. The distance functions of the KNN in equation (6), (7), and (8) are described below:

Euclidean Distance Function

$$D_{FE} = \sqrt{\textstyle\sum_{i=1}^{k}(x_i - y_i)^2} \tag{6}$$

Manhattan Distance Function

$$D_{FM} = \textstyle\sum_{i=1}^{k}|x_i - y_i| \tag{7}$$

Minkowski Distance Function

$$D_{FMI} = \left[\textstyle\sum_{i=1}^{k}(|x_i - y_i|)^q\right]^{\frac{1}{q}} \tag{8}$$

Where, x and y are the features of the dataset. We have

used Euclidean distance function in this work.

Table 1 Normalized value of the PSD of the C4-A1 channel of the EEG signal

EEG Wave	Phase	Max.	Avg.	Min.
Delta	Before	15127.18	44.31781378	0.000000738
	Recitation	32128.84	45.2549673	0.00000295
	After	41782.04	60.683844	0.0000035
Theta	Before	1267.875704	10.37119227	0.000000594
	Recitation	930.3524	10.12340646	0.000000569
	After	1241.47	9.341830491	0.000000361
Alpha	Before	5429.8826	15.175557	0.0000017
	Recitation	4616.132	13.80179011	0.000000191
	After	5341.167	12.981429	0.0000011
Beta	Before	564.91515	20.879796	0.0000019
	Recitation	601.118	20.23	0.00000145
	After	679.5706	19.07039684	0.000000486
Gamma	Before	520.7451879	15.77289635	0.000000738
	Recitation	707.6479	14.21803803	0.000000832
	After	560.2475	13.4547986	0.00000261

4. Results

4.1. Analysis of the signal

We extracted the C4-A1 channel of the EEG signal in the experimental data set. The each segment of the channel are 60 seconds. After segmentation, we used 2048 order Blackman window having finite impulse response filter having sampling frequency are 200 Hz was used to remove the noise of the channel. After filtration, we extracted PSD of the channel as a feature of the C4A1 channel of the EEG signal. Then, we normalized the value of the power spectral density as input of the classifier (Table 1).

4.2. Performance of the proposed system

After PSD as a feature, we applied DT and KNN classifiers having two cross validation model such as 2 and 5 fold for the performance of the system. The standard performance measures are precision, recall, accuracy, and F1 are described in equations (9), (10), (11), and (12).

$$precision = \left(\frac{TP}{TP+FP}\right) \quad (9)$$

$$recall = \left(\frac{TP}{FN+TP}\right) \quad (10)$$

$$accuracy = \left(\frac{(TP+TN)}{TP+TN+FP+FN}\right) \quad (11)$$

$$F1 = 2 \times \frac{recall \times precision}{recall+precision} \quad (12)$$

Table 2 Performance of the proposed system

Fold	Classifier	Precision	Recall	Accuracy	F1
2	DT	0.745	0.745	0.745	0.745
	KNN	**0.970**	**0.970**	**0.970**	**0.970**
5	DT	0.748	0.747	0.747	0.747
	KNN	**0.974**	**0.974**	**0.974**	**0.974**

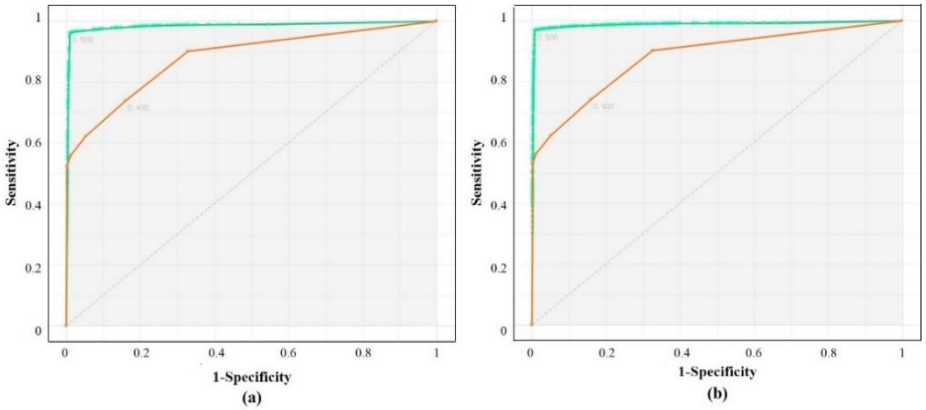


Fig.1 ROC curve for the classification of the proposed system in the cross-validation models such as **(a)** 2 fold and **(b)** 5 fold. It is clear that KNN classifier has highest and DT (brown line) has lowest performance in both cross-validation models.

5. Discussion

After hymn recitation average delta frequency increased prominently which is an indication of deep sleep. This was also an observation in the previous study after *"OM"* hymn meditation [19]. The present study was evaluated both by using KNN and DT classifiers along with the performance of hymn recitation. This finding is also supported by the religious chanting of different religious studies [1]-[3]. Table 2 represented the performance of the proposed system. Our KNN classifier achieved the highest accuracy in both cross-validation models of 2 and 5 fold. The performance of the

KNN classifier having 2 fold cross validation model in terms of precision, recall, accuracy, and F1 was found to be 0.970, 0.970, 0.970, and 0.970, respectively. In addition, the KNN classifier having 5 fold cross-validation model in terms of precision, recall, accuracy, and F1 were found to be 0.974, 0.974, 0.974, and 0.974, respectively. The Receiver Operating Characteristics (ROC) curve for the KNN classifier, holding the highest performance as compared to DT is shown in Figure 1. The limitations of this study are the number of subjects, single gender, and only one feature for analyzing the data. Further study will add more subjects with gender equality to design the system.

6. Conclusions

In this work, we have developed a PSD based model with DT and KNN classification to detect the changes in human brain during recitation of the *maha mrityunjaya hymn*. To be best of our knowledge, this study easily finds the effect in the brain with 97.4% accuracy. Further study will apply this method to the other hymns of the Hindu religious belief.

Acknowledgements

This work was supported by Sichuan Science and Technology Program (2020YJ0225) and CAS Key Laboratory of Mental Health, Institute of Psychology (KLMH2019K04). We would like to thanks all participants of this study. We also acknowledge the Prof. Naseem, Dr. Faez iqbal khan, Miss Mariyam hashmi, and Ijaz gul for useful discussion.

References

[1] H. Doufesh *et al.,* "Effect of Muslim Prayer (Salat) on α Electroencephalography and Its Relationship with Autonomic Nervous System Activity," *J. Altern. Complement. Med.*, 2014.

[2] H. Doufeshet *et al.,* "Effects of Muslims praying (Salat) on EEG gamma activity," *Complement. Ther. Clin. Pract.*, 2016.

[3] H. Doufesh, T. Faisal, K. S. Lim, and F. Ibrahim, "EEG spectral analysis on muslim prayers," *Appl. Psychophysiol. Biofeedback*, 2012.

[4] M. Bin Heyat and M. M. Siddiqui, "Recording of EEG, ECG, EMG Signal," vol. 5, no. 10, pp. 813–815, 2015.

[5] M. B. Bin Heyat, Y. M. Hasan, and M. M. Siddiqui, "EEG signals and wireless transfer of EEG Signals," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 4, no. 12, pp. 10–12, 2015.

[6] R. K. Wallace *et al.,* "A wakeful hypometabolic physiologic state," in *Meditation: Classic and Contemporary Perspectives*, 2017.

[7] B. Gangadhar *et al.*, "Neurohemodynamic correlates of ′OM′ chanting: A pilot functional magnetic resonance imaging study," *Int. J. Yoga*, 2011.

[8] N. P. Rao *et al.*, "Directional brain networks underlying OM chanting," Asian *J. Psychiatr.*, 2018.

[9] B. P. Harne and A. S. Hiwale, "EEG Spectral Analysis on OM Mantra Meditation: A Pilot Study," *Appl. Psychophysiol. Biofeedback*, 2018.

[10] M. B. Bin Heyat, F. Akhtar, M. Ammar, B. Hayat, and S. Azad, "Power Spectral Density are used in the Investigation of insomnia neurological disorder," in *XL- Pre Congress Symposium*, 2016, pp. 45–50.

[11] M. B. B. Heyat *et al.,* "Short Time Frequency Analysis of Theta Activity for the Diagnosis of Bruxism on EEG Sleep," in *Advanced Computational Intelligence Techniques for Virtual Reality in Healthcare. Studies in Computational Intelligence*, K. Gupta D., Hassanien A., Ed. Springer, 2020, pp. 63–83.

[12] M. B. Bin Heyat *et al.*, "Bruxism Detection Using Single-Channel C4-A1 on Human Sleep S2 Stage Recording," in *Intelligent Data Analysis: From Data Gathering to Data Comprehension*, 1st ed., D. Gupta, S. Bhattacharyya, and A. Khanna, Eds. John Wiley & Sons, 2020, pp. 347–367.

[13] M. B. Bin Heyat *et al.*, "Normalized Power are used in the Diagnosis of Insomnia Medical Sleep Syndrome through EMG1-EMG2 Channel," *Austin J. Sleep Disord.*, vol. 4, no. 1, pp. 2–4, 2017.

[14] M. B. Bin Heyat, *Insomnia: Medical Sleep Disorder & Diagnosis*, 1st ed. Hamburg, Germany: Anchor Academic Publishing, 2016.

[15] D. Lai, M. B. Bin Heyat, F. I. Khan, and Y. Zhang, "Prognosis of Sleep Bruxism Using Power Spectral Density Approach Applied on EEG Signal of Both EMG1-EMG2 and ECG1-ECG2 Channels," *IEEE Access*, vol. 7, pp. 82553–82562, 2019.

[16] M. B. Bin Heyat *et al.*, "Sleep Bruxism Detection Using Decision Tree Method by the Combination of C4-P4 and C4-A1 Channels of Scalp EEG," *IEEE Access*, vol. 7, pp. 102542–102553, 2019.

[17] G. Ke *et al.*, "LightGBM: A highly efficient gradient boosting decision tree," 2017.

[18] L. Peterson, "K-nearest neighbor," *Scholarpedia*, 2009,

[19] B. P. Harne, Y. Bobade, R. S. Dhekekar, and A. Hiwale, "SVM classification of EEG signal to analyze the effect of OM Mantra meditation on the brain," 2019.

METHOD OF SAFETY HELMET WEARING DETECTION BASED ON KEY-POINT ESTIMATION WITHOUT ANCHOR

DUAN QIPENG[1], KUANG PING [1], LI FAN[1], HE MINGYUN[1], GAO YU[1]

School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
E-MAIL: duanqipeng@foxmail.com, kuangping@uestc.edu.cn

Abstract:

Safety Helmet wear detection is a very important task in the field of industrial applications which can greatly reduce the safety risk and provide a guarantee for better industrial production. Most of the popularly used detection methods realized by enumerating all the possible locations of detection objects, the classifier is then run to identify the final rectangular bounding box that wraps the target and the category to which it belongs. In this paper, we design a multi-scale key-point network to solve the size difference of the objects, coming up with a new loss function and training strategy to improve the accuracy of the result. Our method achieves 100 FPS 92% mAP on the SHWD dataset, which achieves the best trade-off between speed and accuracy.

Keywords:

Key-point Estimation; Helmet wearing detection; Industry landing application; Objection detection;

1. Introduction

The basic goal of the object detection task is to demarcate the position of the object to be detected in the image and correctly distinguish the class of the object. As a cornerstone of computer vision research, it is to solve problems such as instance-segmentation [1], scene Content perception, object tracking [2], event recognition, and other more complex task foundation, because of its universal value and academic attention. With the development of deep learning, the application of deep convolutional neural network, which can extract high dimensional features from images, makes the research of object detection into a new level in a short time. It is the main trend that academia and industry combine closely and promote each other. But it can't be ignored that the focus on the algorithm itself between the academia and Industry Complex application scenario is still difficult to achieve efficient compatibility. In this paper, we provide a simple, efficient, and accurate detection implementation for helmet wearing, a common industrial security task. Our detector is based on the key-point estimation method [3,5], which is different from the traditional bounding box with an anchor box. Corresponding to the scene characteristic of helmet wearing, we improved the key-point estimation network to generate the fine heat map and then extracted the peak point of the class heat map for each image as the center point of the bounding box we located, the regression produces other properties of the center point corresponding to the object.

Our method is robust and scene-compatible, and the specific network design and the whole pipeline process make the algorithm maintain a high accuracy rate based on realizing high-speed detection, a 100FPS 92% mAP is obtained on the industry open-source dataset SHWD, which achieve faster reasoning and more accurate identification compared with the industry optimal algorithm.

2. Related work

DCNN. Multi-layer neural networks have become more and more mature after years of precipitation. Conventional fully connected neural networks have poor performance in image representation and are difficult to extract high-dimensional features of images, the deep neural network structure based on convolution computation emerges as the Times require. The Deep convolutional neural network can reliably aggregate local perceptual domain features with minimal computational effort, and shared weighted network features can greatly encode the structural features of the space to which they belong, this provides strong support for the generalization of input. Our approach is based on the idea of a full-convolutional neural network taking into account the DCNN's inability to achieve pixel-level awareness, through a full-convolutional neural network, we were able to input an image into the network and then output a precise

point heat map, which effectively enhanced the detector's sensitivity to the image and provided a solution for better key-point estimation.

Object Detector base on anchor. At the beginning of deep learning in the field of object detection, a two-stage detector is the main method to realize it [7,8,12], in the initial stage, all possible positions of the object in the input image are exhausted to prepare sample points for the subsequent stage, which is often referred to as the proposal box, this stage can be accomplished by traditional Algorithms or specific neural networks. To improve the performance of the network, the idea of anchor frame is put forward, and the anchor frame with different length-width ratio and multi-scale is generated by using the anchor mechanism in the sliding window to better meet the needs of covering objects of different sizes like YOLOv3 [4], the invention effectively solves the generating malpractice of the inefficient proposal box. In this paper, we use a method similar to the traditional single-stage object detection, which can be called anchor-free estimation, it encodes the position of the object without paying attention to the overall coverage of the object; for each object, there is only one key point that can be produced, this avoids the NMS post-processing operations [5,11]. we specially designed the key point estimation network to generate a larger feature convolution graph to solve the scale problem

Key-point estimation. In the research of object detection realization theory, the detection algorithm based on the estimation of key points is not new, the conventional detection can be realized based on corner points, for example, CornerNet [5] has predicted three points for each target in the realization, they are upper left, the bottom right, and the center point, and after the generation of re-grouping, the point and the object one-to-one correspondence. However, the dense and small-scale scene characteristics make the generation of grouping and point messy and rough, which can't meet the requirement of high accuracy, therefore, we adopt center point estimation [3], only focus on the single center of an object, avoid grouping conflict, and improve the application reliability of the algorithm.

3. Method

A good algorithm for the industrial scene should combine the task characteristics closely and encode the potential prior information completely to help the algorithm produce correct output to any input in the application. In this paper, we fully consider the characteristics of this industry, and integrate the scene information into the Algorithm's design.

3.1. Backbone

In this section, we describe in detail the backbone network structure (Fig.1) used to generate the key-points of an object.

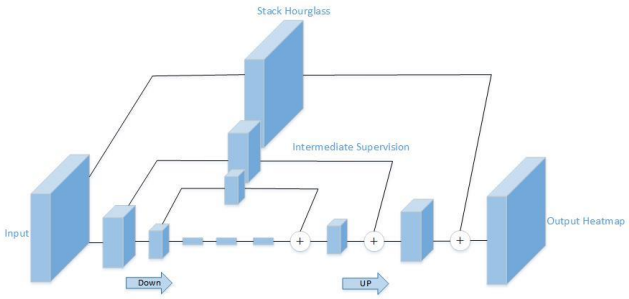


Fig.1 Stack Hourglass with three stacks

The basic network structure used in this paper is the stack hourglass network structure [6]. The basic component of the network is a residual module, which uses a jumper to add by-pass, and splices the low-dimension feature and the high-dimension feature to encode the image information better. The key design of the hourglass network is the structure of its sub-network. Before each down-sampling, the original scale information is reserved in the upper half, and after each up-sampling, the data of the previous scale is added which makes scale information of the superposed image feature map is rich and the information loss is minimal. We reduce the number of network stacks which increased the output feature size by 1.5 times.

3.2. Mapping of GT

We use the normal Gaussian kernel [5] to scatter the GT points on the feature map. For the corresponding object on the image (X, Y), according to the Gaussian kernel, the calculation radiates to the surrounding with this point as the center, the center value being 1, in this way, the closer to the center on the thermodynamic chart, the closer it is to 1, the farther it is to 0. When the thermodynamic charts overlap, simply take the maximum value.

3.3. Design of Loss Function

Confidence loss. We follow the philosophy of Focal loss and make some targeted improvements based on the helmet-wearing scenario. Because of the imbalance of positive and negative samples in the open-source data set and the big difference in the size of the objects to be tested, we add the judgment condition of the prediction value to increase the penalty of the loss when the network prediction has a big error. In the formula, $Yxyc$ represents the

confidence level of GT, $\hat{Y}xyc$ represents the predicted value of the network, N is the number of key-points in GT with value 1, which is normalized. Alpha and Beta are the super-arguments to Focal loss [9], which we set to 3 and 4 in this article. Here is the formulation.

$$\frac{1}{N}\sum_{xyc}\begin{cases}\left(1-\hat{Y}xyc\right)^{\alpha} log\left(\hat{Y}xyc\right) if\ Yxyc=1 \\ (1-Yxyc)^{\beta}\left(\hat{Y}xyc\right)^{\alpha} log\left(1-\hat{Y}xyc\right) if\ 0.2<Yxyc \\ (1-Yxyc)^{\frac{\beta}{2}}\left(\hat{Y}xyc\right)^{\sqrt{\alpha}} log\left(1-\hat{Y}xyc\right) if\ Yxyc<0.2\end{cases} \quad (1)$$

Floating-point offset loss. In this paper, stride = 3 is used to scale the input image (R = 3), this will result in a certain precision error when the feature map after convolution is resampled back to the original image (for example, there is only a one-pixel difference on the feature map due to the floating-point loss of down rounding and up rounding, which corresponds to the difference of three pixels on the original map), so for each center point, an offset error is used to correct it. where $\frac{l}{R}$ uses the lower sampling to get the GT position, $\tilde{l}$ is the downward integral coordinate position of the Pixel position, and $\hat{o}_{\tilde{l}}$ is the predicted offset value.

$$L_{offset}=\frac{1}{N}\sum_{l}\left|\hat{o}_{\tilde{l}}-\left(\frac{l}{R}-\tilde{l}\right)\right| \quad (2)$$

Object size loss. Where s_o is the size of the object, and is calculated by:

$$s_o=\left({x_2}^{(o)}-{x_1}^{(o)},{y_2}^{(o)}-{y_1}^{(o)}\right) \quad (3)$$

which is calculated before the neural network is trained, to reduce the computation and the difficulty of Network Regression, stride = 3 is used to calculate the length and width of the sample. Considering the small target size problem in the scene, L2 distance is used to further improve the penalty level in case of error.

$$L_{size}=\frac{1}{N}\sum_{o=1}^{N}\left|\hat{S}_{l_o}-s_o\right|^2 \quad (4)$$

4. Experiment

4.1. Dataset

The training and testing dataset of this paper are all carried out on SHWD, which is an open-source data set about helmet wearing and head detection. It contains 7,581 images, including 9,044 positive helmet wearing samples and 111514 negative helmet wearing samples in VOC style [10]. SHWD has strict requirements on data classification, for example, non-safety Helmet data such as people wearing hats are labeled as negative samples, which has very realistic classification significance. The images are from Google, Baidu, and SCUT-HEAD, all of which are tagged in VOC format.

4.2. Training details

In this experiment, we used the popular technology of multi-image combination, spliced the images of different scenes according to the reasonable logic, and formed a new scene image. At the same time, we also used the conventional image enhancement method, include classical geometry and optical variations, random occlusion, and blur processing techniques. In designing our training strategy, we paid particular attention to the idea of transfer learning, so we innovatively trained the network first on a pure head dataset BrainWash and then on an SHWD dataset after pre-training the 100epoch, through this training strategy, we are surprised to find that the accuracy of the model has been significantly improved, and training stability and speed has been improved. The input resolution is 768 * 768, the output tensor is 256 * 256 after network calculation. NVIDIA GTX 2080Ti GPUS has been trained for 140 rounds. The network is optimized by using Adam optimizer. The initial learning rate is set to 0.001, round 80 set at 0.0001, round 120 set at 0.00001. The whole training process takes three days.

4.3. Result

The output of the model is shown in Fig.2, Fig.3 The single image processing time is only 0.01 second.

Fig.2 Simple background result

Fig.3 Complicated background result

We also compared the results with Yolov3 and conventional key-point CenterNet(Fig.4). It is clear that the model has good generalization ability and precision for small

scale and complex background, which is the best Algorithm of the current security helmet wear detection task.

YOLOv3 CenterNet Our Model

Fig.4 Comparison results

4.4. Test and verify

High real-time and accurate safety helmet wear detection can greatly reduce the cost on the security of human, the significance of safety production is extraordinary, our method achieves the highest accuracy under the same detection speed of the same kind of scene algorithm. The following is a quantitative comparison table of performance parameters.

Table 1 Performance comparison

	AR	mAP	Average speed
Faster-RCNN	80%	85%	15FPS
YOLOV3 [8]	85%	88.5%	50FPS
CenterNet [3]	90%	90%	90FPS
Our Model	95%	92%	100FPS

We selected the highest number of processing frames, average precision, and average recall to compare the performance of different algorithms. As can be seen from the table, our algorithm achieves the best results in all three accepted metrics.

5. Conclusion

In this paper, considering the particularity and complexity of the detection task, an end-to-end security helmet-wearing detection algorithm based on scenario correlation is proposed, we achieve the best recognition and accuracy performance under the same real-time condition. After extensive real-world testing, the effectiveness of our algorithm is verified.

Acknowledgments

This work supported by Sichuan Science and Technology Program (2019ZDZX0005、2020YFG0309)

References

[1] Y. Li, H. Qi, J. Dai, X. Ji, and Y. Wei. Fully convolutional instance-aware semantic segmentation. In CVPR, 2017.

[2] Z. Kalal, K. Mikolajczyk, and J. Matas. Tracking learning-detection. TPAMI, 2012.

[3] Xingyi Zhou, Dequan Wang, Philipp Krähenbühl Object as points. In CVPR, 2019.

[4] J.Redmon and A.Farhadi. Yolov3: An incremental improvement. arXiv preprint arXiv:1804.02767, 2018.

[5] H. Law and J. Deng. Cornernet: Detecting objects as paired keypoints. In ECCV, 2018.

[6] A. Newell, K. Yang, and J. Deng. Stacked hourglass networks for human pose estimation. In ECCV, 2016.

[7] W. Liu, D. Anguelov, D. Erhan, C. Szegedy, S. Reed, C.-Y. Fu, and A. C. Berg. SSD: Single shot multibox detector. In ECCV, 2016.

[8] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi. You only look once: Unified, real-time object detection. In CVPR, 2016.

[9] Tsung-Yi Lin, Priya Goyal, Ross Girshick, Kaiming He, Piotr Dollár. Focal loss for dense object detection. ICCV, 2017.

[10] M. Everingham, L. Van Gool, C. K. I. Williams, J. Winn, and A. Zisserman. The PASCAL Visual Object Classes Challenge 2012 (VOC2012) Results.

[11] Alexey Bochkovskiy, Chien-Yao Wang, Hong-Yuan Mark LiaoYOLOv4: Optimal Speed and Accuracy of Object Detection

MM-GCN: MULTI-MUTUAL LEARNING NETWORKS OF GRAPH CONVOLUTION FOR NODE CLASSIFICATION

GAO YU [1], KUANG PING[1], HE MINGYUN[1], DUAN QIPENG[1], LIU CHENYANG[1]

[1]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China
E-MAIL: YuTesla@outlook.com, kuangping@uestc.edu.cn

Abstract:

Graph Convolutional Network (GCN) has been proved to be an effective method to process graph-structured data. Concurrently, deep mutual learning has shown significant improvements in network performance. In this paper, we propose a model: Multi-Mutual learning Networks of GCN(MM-GCN), which combines these two lines of work. At its core, MM-GCN trains multiple GCNs, which may be the same or different, and the final loss function is jointly determined by these networks, which can be used for backpropagation to train the network. Our experiments show that the effect of MM-GCN proposed by us improves state-of-the-art baselines on node classification tasks.

Keywords:

Tracking; Graph Convolutional Network; Deep mutual learning; Node classification

1. Introduction

Graphs are important non-Euclidean structural data that can be modeled by a set of nodes(objects) and edges(relationships). In recent years, due to the powerful representation of graphs, which can be used in social science (social networks), natural science (physical systems and protein-protein interaction networks), knowledge graphs, and many other research areas [1], more and more scholars have paid attention to the use of machine learning methods to analyze graph data.

The convolutional neural network has achieved great success in processing Euclidean structural data (such as images, videos) [2]. It is natural to wonder whether the operation of convolution can be applied to the graphs. However, the core of the convolution operation is to maintain translation invariance. However, non-European data does not have translation invariance [3]. There are only two ways to solve this problem:

1.Find a kernel that can process non-Euclidean data

2.Map non-Euclidean data to Euclidean space for processing

The spatial domain approach is the first approach, while the spectral domain approach is the second approach.

Our approach is mainly based on the latter. in this work, we start multiple networks. During the process of training, these networks learn from each other. In each iteration, we calculate the predictions of the multiple networks, and update the networks according to the results of those models, until convergence.

2. Related work

Non-spectral approaches define convolutions directly on the graph, operating on spatially close neighbors. The main challenge of this approach is to define convolution operations of different sizes without losing local invariance.

DCNN [4] proposed the diffusion-convolutional neural network (DCNN), which defines a hop matrix for each node, denoted as P^n. For node N, its h-hop node is the node that can be reached after h steps starting from node N. The node classification task can be calculated by the following formula:

$$\mathbf{H} = f(\mathbf{W}^c \odot \mathbf{P}^* \mathbf{X}) \tag{1}$$

where $\mathbf{X} \in {}^{N \times F}$ is the input feature matrix (N is the number of nodes and F is the number of features). $\mathbf{P}^*$ is an $N \times K \times N$ tensor that contains the power series $\{\mathbf{P}, \mathbf{P}^2, ..., \mathbf{P}^K\}$ of $\mathbf{P}$, which is the degree-normalized transition matrix from the adjacency matrix $\mathbf{A}$. $\mathbf{P}^* \mathbf{X}$ represents the information after K-hops of the node's F-dimensional feature diffusion. Finally, these features are aggregated by the Hadamard product.

Graph attention network (GAT) [5] uses the attention mechanism, through which the convolution function is defined. The graph sampling aggregation network (GraphSAGE) [6] also implements the spatial domain method by defining the convolution function by sampling the adjacent nodes randomly.

The spectral domain convolution defines the Fourier transform on the graph domain and simplifies the calculation

by the eigendecomposition of the Laplace matrix.

Spectral Network [7] defines the convolution operation in spectral-domain by convolution theorem on graph space:

$$\mathbf{g_\theta} *_G \mathbf{x} = \mathbf{U}\mathbf{g_\theta}(\Lambda)\mathbf{U}^T\mathbf{x} \tag{2}$$

where $\mathbf{g_\theta}$ is the kernel, $\mathbf{x}$ is the input, $*_G$ is the convolution operation in the spectral domain. $\mathbf{U}$ is the matrix of eigenvectors of the normalized graph Laplacian matrix $\mathbf{L} = \mathbf{I_N} - \mathbf{D}^{-\frac{1}{2}}\mathbf{A}\mathbf{D}^{-\frac{1}{2}} = \mathbf{U}\Lambda\mathbf{U}^T$. Where $\mathbf{A}$ is the adjacency matrix of the graph and $\mathbf{D}$ is the degree matrix of $\mathbf{A}$, Λ is the eigenvalue matrix of $\mathbf{L}$.

ChebyNet [8] uses truncated Chebyshev polynomials $\mathbf{T}_k(x)$ to approximate $\mathbf{g_\theta}(\Lambda)$:

$$\mathbf{g_\theta} *_G \mathbf{x} \approx \sum_{k=0}^{K} \theta_k \mathbf{T}_k(\mathbf{L})\mathbf{x} \tag{3}$$

where $\mathbf{L} = \frac{2}{\lambda_{\max}}\mathbf{L} - \mathbf{I_N}$, $\lambda_{\max}$ is the largest eigenvalue of $\mathbf{L}$. Thus, we do not need to compute the eigenvectors of the Laplacian.

GCN [9] set the K to 1 and approximated $\lambda_{\max}$ to 2, thus the equation simplifies to:

$$\mathbf{g_\theta} *_G \mathbf{x} \approx \theta_0'\mathbf{x} + \theta_1'(\mathbf{L} - \mathbf{I_N})\mathbf{x} = \theta_0'\mathbf{x} - \theta_1'\mathbf{D}^{-\frac{1}{2}}\mathbf{A}\mathbf{D}^{-\frac{1}{2}}\mathbf{x} \tag{4}$$

with two parameters θ_0' and θ_1'. We can get the following expression by setting $\theta = \theta_0' = -\theta_1'$:

$$\mathbf{g_\theta} *_G \mathbf{x} \approx \theta(I_N + \mathbf{D}^{-\frac{1}{2}}\mathbf{A}\mathbf{D}^{-\frac{1}{2}})\mathbf{x} \tag{5}$$

Using a renormalization trick:

$$\mathbf{I}_N + \mathbf{D}^{-\frac{1}{2}}\mathbf{A}\mathbf{D}^{-\frac{1}{2}} \rightarrow \mathbf{D}^{-\frac{1}{2}}\mathbf{A}\mathbf{D}^{-\frac{1}{2}} \tag{6}$$

with $\mathbf{A} = \mathbf{A} + \mathbf{I_N}$ and $D_{ii} = \sum_j A_{ij}$, we get the final feature maps:

$$\mathbf{H}^{(i+1)} = \sigma(\mathbf{A}\mathbf{H}^{(i)}\mathbf{W}^{(i)}) \tag{7}$$

with $\mathbf{A} = \mathbf{D}^{-\frac{1}{2}}\mathbf{A}\mathbf{D}^{-\frac{1}{2}}$, where $\mathbf{H}^{(i)}$ and $\mathbf{H}^{(i+1)}$ are the input and output for layer i. $\mathbf{W}^{(i)}$ is a trainable weight matrix, theta is an activation function.

3. Method

3.1. Network Architecture

Our MM-GCN is a multi-network structure, with two subnetworks as an example (see Figure 1). It is also natural to extend to multiple networks, as shown in 3.3. For a task, start training with two identical or different networks called student networks [10]. After the predicted value of the two networks is generated, we calculate the KL divergence of the two networks and add to the final loss function. Then do backpropagation and update the weights.

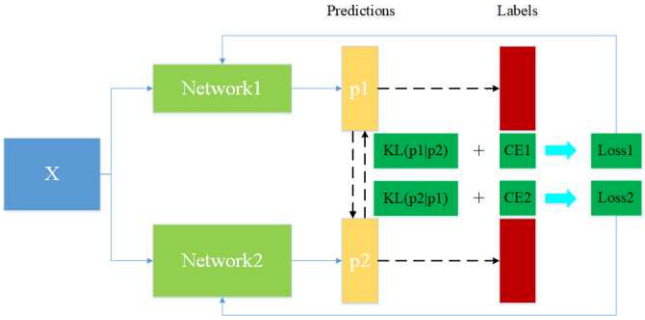


Fig.1 Network Architecture

3.2. Loss Function

We donate the probability of the sample x_i belongs to class **m** which is given by network 1 as $p_1^m(x_i)$:

$$p_1^m(x_i) = \frac{\exp(z_1^m)}{\sum_{m=1}^{M}\exp(z_1^m)} \tag{8}$$

where z_1^m is the output of the softmax layer of network 1.

The total loss function is composed of two parts, one is the cross-entropy function, the other is the KL divergence loss.

The cross-entropy function calculates the cross-entropy error between the predicted value of the network and the true labels:

$$L_{C_1} = -\sum_{i=1}^{N}\sum_{m=1}^{M} I(y_i, m)\ln(p_1^m(x_i)) \tag{9}$$

where $I(y_i, m)$ is indicator function defined as:

$$I(y_i, m) = \begin{cases} 1 & y_i = m \\ 0 & y_i \neq m \end{cases} \tag{10}$$

KL divergence can be used to measure the matching degree between two distributions. Since the true value is the same, it is natural that we expect the prediction results of the two student networks to be the same.

The KL divergence from p_1 to p_2 is calculated as:

$$D_{KL}(p_2 \| p_1) = \sum_{i=1}^{N}\sum_{m=1}^{M} p_2^m(\mathbf{x}_i)\ln\frac{p_2^m(\mathbf{x}_i)}{p_1^m(\mathbf{x}_i)} \tag{11}$$

The KL divergence from p_1 to p_2 is calculated as:

$$D_{KL}\left(p_1 \| p_2\right)=\sum_{i=1}^{N}\sum_{m=1}^{M} p_1^m\left(\mathbf{x}_i\right)\ln\frac{p_1^m\left(\mathbf{x}_i\right)}{p_2^m\left(\mathbf{x}_i\right)} \tag{12}$$

The total loss function of network 1 is defined as:

$$L_1 = L_{C_1} + \kappa D_{KL}(p_2 \| p_1) \tag{13}$$

where κ is the KL weight to control the KL loss. Similarly, the total loss function of network 2 is defined as:

$$L_2 = L_{C_2} + \kappa D_{KL}(p_1 \| p_2) \tag{14}$$

It should be noted that KL divergence is asymmetric, in general, $D_{KL}(p_1 \| p_2) \neq D_{KL}(p_2 \| p_1)$. So the values calculated by these two loss functions are not the same.

3.3. Extension to More Student Networks

3.1 and 3.2 describe how MM-GCN is learned in the case of two student networks. MM-GCN can also be extended to multiple student networks.

Given N student networks (N>=2), the loss function of the network n. The cross-entropy loss function is unchanged, while the KL loss function can calculate the KL divergence of network N from other N-1 networks respectively, and then calculate the average value:

$$L_k = L_{C_k} + \kappa\frac{1}{N-1}\sum_{l=1,l\neq k}^{N} D_{KL}\left(p_l \| p_k\right) \tag{15}$$

The extended multi-network structure here can use the same network or different networks under the same task. Different networks may achieve better results. Detailed information is discussed in section 4.

3.4. Experiments and Results

In this section, we will introduce the training and test results of our model on the Cora dataset and compare the results with GCN [9]. Specific experimental steps and results are as follows:

3.5. Datasets

We train models on the classic citation network dataset: Cora. Cora contains 2708 articles published in the journal of corresponding papers, each paper has a category as a tag, Cora contains sparse bag-for-words feature vector of each paper and a list of citation relations between papers. We set the relationships as (undirected) edges and papers as nodes, to construct a binary adjacency matrix as the input of the network.

3.6. Parameters Setting

We implement all network and train models in Torch and conduct all experiments on the NVIDIA GeForce GTX 1050Ti GPU. We use [9] as the baseline and adopted the experimental settings used by Kipf in the paper. Specifically, we train our models using Adam optimizer for a maximum of 200 epochs, with an initial learning rate of 0.01 that decays by 0.01 percentage. We use L2 regularization on the weights with a dropout rate of 0.5 and set the KL weight as 1. GCNs with hidden layers of 18, 36, and 54 neurons are trained as the baseline. We noticed that the Cora dataset is sensitive to initializations, so we trained all models 50 times, and report the average value of the top 20 accuracy rates as the final accuracy rates.

3.7. Results and Comparing

Table 1 compares the accuracy of the various architectures of the MM-GCN with double student networks on the Cora dataset. From this table, we can draw the following conclusions: (i) All different network combinations of GCN-18, GCN-36 and GCN-54 improve the performance compared to learning independently, indicated by the all positive values in the "MM-GCN vs Independent" columns; (ii) Although GCN-54 is a much larger network than GCN-18, it is improved by learning from a smaller peer; (iii) Usually, networks with different structures are put together to learn from each other and get more improvements than those with the same structure.

Table 1 Average accuracy (%) on the Cora dataset of MM-GCN with double student networks

Network Types		Independent		MM-GCN		MM-GCN vs Independent	
Net 1	Net 2	Net 1	Net 2	Net 1	Net 2	Net1	Net 2
GCN-18	GCN-18	82.92	82.92	83.02	83.40	0.10	0.48
GCN-18	GCN-36	82.92	83.06	83.03	83.36	0.11	0.30
GCN-18	GCN-54	82.92	83.10	83.46	84.50	0.54	1.40
GCN-36	GCN-54	83.06	83.10	83.64	84.20	0.58	1.10

GCN-36	GCN-36	83.06	83.06	83.84	83.74	0.78	0.68
GCN-54	GCN-54	83.10	83.10	83.69	83.59	0.59	0.49

Table 2 Average accuracy (%) on the Cora dataset of MM-GCN with 10 student networks

Network Types	Independent	MM-GCN	MM-GCN vs Independent
GCN-18	82.92	83.51	0.59
GCN-36	83.06	83.72	0.66
GCN-54	83.10	84.05	0.95

Table 2 compares the accuracy of MM-GCN with multiple student networks (each MM-GCN trains 10 networks with the same structure) on the Cora dataset (the accuracy of MM-GCN is the average of the accuracy of each student network). From the table we can make the following observations: (i) Training a group of MM-GCN with the same structure can still improve the accuracy compared with independent learning; (ii) More improvement was achieved by training multiple groups of MM-GCN than by training only two groups of MM-GCN.

4. Conclusion

In this paper, we propose a new graph convolutional neural network architecture based on mutual learning, and design a citation network classification model based on Torch deep learning framework. In the experiment, we used Cora dataset to train our model and GCN with different structures. The results show that this method can improve the performance of small networks, and more complex networks can benefit from mutual learning with small networks. Even networks with the same architecture can be significantly improved when the number of student networks is large enough.

Acknowledgments

This work is supported by the Sichuan Science and Technology Program (2020YFG0309、2020GFW068、2020ZHCG0058、2019ZDZX0005).

References

[1] Zhou, J., Cui, G., Zhang, Z., Yang, C., Liu, Z., & Sun, M. “Graph neural networks: A review of methods and applications”, arXiv:1812.08434, 2016.

[2] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, “Gradient-based learning applied to document recognition”, Proceedings of the IEEE, vol. 86, no. 11, pp. 2278–232, 1998.

[3] F. Wu, A. Souza, T. Zhang, C. Fifty, T. Yu, and K. Weinberger, “Simplifying graph convolutional networks,” in International Conference on Machine Learning, 2019.

[4] J. Atwood and D. Towsley, “Diffusion-convolutional neural networks”, NIPS 2016, pp. 1993–2001, 2016.

[5] P. Velickovic, G. Cucurull, A. Casanova, A. Romero, P. Lio, and Y. Bengio, “Graph attention networks”, ICLR 2018, 2018.

[6] W. L. Hamilton, Z. Ying, and J. Leskovec, “Inductive representation learning on large graphs”, NIPS 2017, pp. 1024–1034, 2017

[7] J. Bruna, W. Zaremba, A. Szlam, and Y. Lecun, “Spectral networks and locally connected networks on graphs”, ICLR 2014, 2014.

[8] D. K. Hammond, P. Vandergheynst, and R. Gribonval, “Wavelets on graphs via spectral graph theory”, Applied and Computational Harmonic Analysis, vol. 30, no. 2, pp. 129–150, 2011.

[9] T. N. Kipf and M. Welling, “Semi-supervised classification with graph convolutional networks,” ICLR 2017, 2017.

[10] Y. Zhang, T. Xiang, T. M. Hospedales, and H. Lu. “Deep mutual learning”, arXiv preprint arXiv: 1706.00384, 2017.

3D SHAPE RECONSTRUCTION OF FURNITURE OBJECT FROM A SINGLE REAL INDOOR IMAGE

LI XI[1], KUANG PING[1], GU XIAOFENG[1], HE MINGYUN[1]

[1]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
E-MAIL: xi-li@foxmail.com, kuangping@uestc.edu.cn, guxf@uestc.edu.cn, hmyun@uestc.edu.cn

Abstract:

Most of the current researches on 3D shape reconstruction based on deep learning only focus on clean-background images. In this paper, we propose a system that segments furniture object from a single real indoor image and reconstructs their 3D meshes. This system takes Pixel2Mesh, a 3D shape reconstruction network, as a branch of the state-of-the-art instance segmentation network Mask Scoring R-CNN. We trained our system on 3D-FUTURE dataset, and the results show that our method can effectively reconstruct 3D shape of furniture objects from real indoor images by designing proper loss functions and combining instance segmentation and 3D shape reconstruction network.

Keywords:

3D shape reconstruction; Real indoor image; Furniture object; Deep learning; Instance segmentation

1. Introduction

Due to the interference of complex background, slightly occluded or partial absence, it is difficult to reconstruct 3D shapes of furniture object from a single real indoor image. At present, most of the researches about three-dimensional shape reconstruction focus on images without background.

We propose a system, which equips a 3D reconstruction branch to the instance segmentation network MS R-CNN [6]. This branch takes the region feature of each target object as the inputs of the three-dimensional shape reconstruction network Pixel2Mesh(P2M) [1], and outputs the 3D mesh of the object by deforming an original sphere. In general, the input of this system is real-world RGB images containing furniture objects, and the outputs are the category, bounding box, mask and three-dimensional mesh of furniture objects.

We trained our system on 3D-FUTURE [5], a large real indoor scenes dataset released by Alibaba. The experimental results show this system can effectively reconstruct the 3D shape of furniture objects in single real indoor scenes images.

The contributions of this paper are highlighted as follows:

• Designing a system that can reconstruct 3D mesh of furniture objects from single view real indoor RGB images quickly and cheaply.

• Designing loss functions for this system properly.

2. Related works

2.1. Traditional modeling from images

Most traditional modeling methods focus on multi-view such as using 3D reconstruction software like Meshroom, 3D models can be generated with high resolution based on the Alice Vision Photogrammetric Computer Vision framework. It infers the geometry of a scene from a set of unordered photographs or videos.

These methods need multiple images of objects and spend a lot of time for professional designers to obtain accurate 3D models. Ideally, people expect three-dimensional CAD models can be modeled from a single real-world image quickly and cheaply.

2.2. Instance segmentation

Instance segmentation network Mask R-CNN [3], a learning-based method, extends the object detection network to get regions of object instances, and then give masks for every region. MS R-CNN [6] moves further forward, it adds a MaskIoU branch for mask score based on mask head, which solves the potential problem of Mask R-CNN only using classification score to measure mask quality.

2.3. Learning-based 3D shape reconstruction

In recent years, neural-network researchers have proposed a variety of forms of 3D representations based on deep-learning methods and computer graphics.

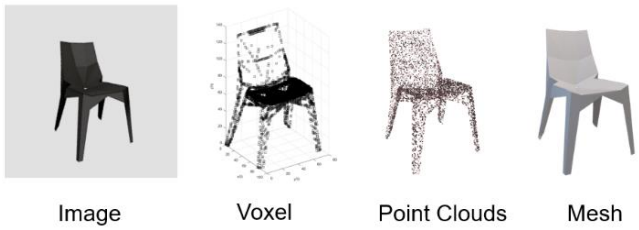


Fig.1 3D representations

3D-R2N2 [6] reconstruct 3D voxels from single or multiple pictures end-to-end; besides, there are methods based on point cloud representation, such as PSG [1], attempts to reconstruct 3D shape from RGB or RGB-D images. Moreover, Pixel2Mesh [1], based on triangular mesh representation, uses Graph Convolution Network (GCN) to represent 3D mesh information, and gradually deforms the ellipsoid mesh by using the features, which extracted from the input RGB image, to generate the desired 3D geometry shape. These methods only focus on the clean-background images.

2.4. Datasets

ShapeNet [8] is a large three-dimensional CAD model dataset, whose 3D CAD are rendered to generate synthetic pictures. Pix3D [3] is a single-image 3D shape modeling dataset, which provides more accurate 2D-3D alignment for 395 3D shapes of 9 object categories. Lately, Alibaba released 3D-FUTURE [5], which contains more than twenty thousand realistic synthetic images in 5,000+ different tidy indoor scenes. These images involve more than ten thousand unique industrial three-dimensional instances of furniture object with high-resolution information-rich textures developed by a bunch of professional designers.

3. Methods

3.1. Network architecture

The instance segmentation network MS R-CNN consists of 2 branches. R-CNN Branch is responsible for the object detection task and outputs the classification results and bounding boxes of the detected objects, while the Mask/MaskIoU Branch is responsible for the instance segmentation task and outputs the masks and mask scores of the target objects.

As shown in Figure 2, we augment MS R-CNN with P2M as a Shape Deformation Branch, which uses an ellipsoid mesh with 156 vertices and 462 edges as the initial shape of any objects, and then gradually uses the 2D image features to adjust the node state of the Graph Convolution Network in 3D mesh to deform the ellipsoid into a target object mesh with 2562 vertices and 5120 faces. Instead of using the feature maps from different layers of VGG in [4], we take ResNeXt-101 and FPN as our feature-extractor and use feature maps resulting from RoIAlign to feed the Shape Deformed Branch.

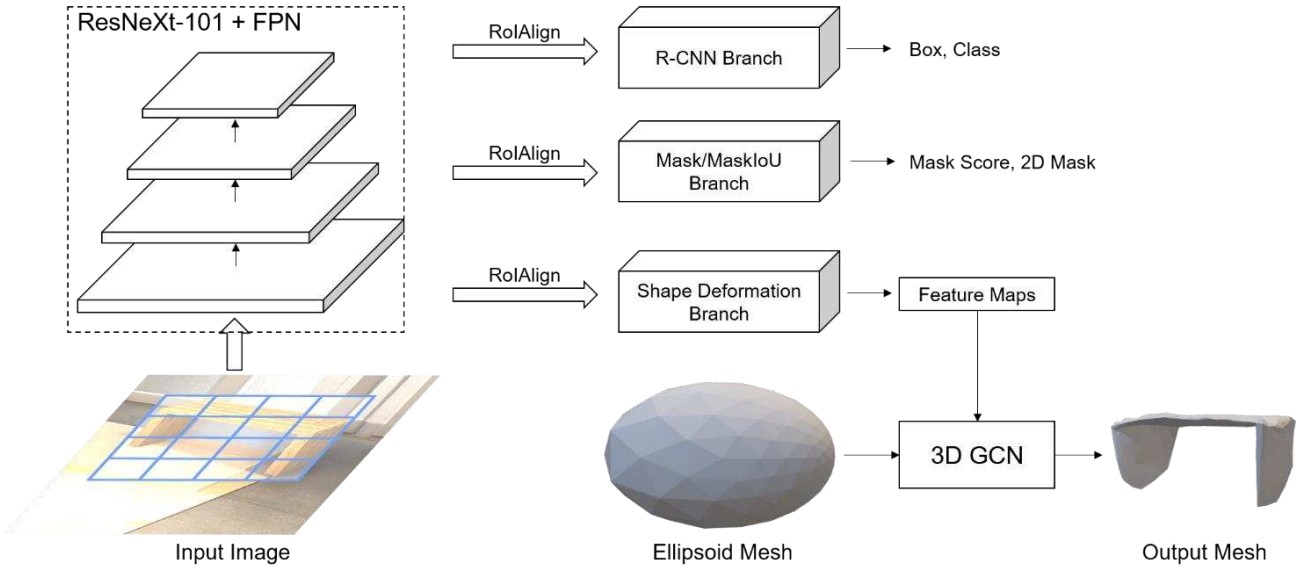


Fig.2 Network architecture

3.2. Loss functions

We properly design the loss functions for our system. X and Y are defined as the point clouds uniformly sampled from the surface of the output mesh and the ground truth mesh. The chamfer distance is used to improve the similarity between X and Y, which is given by

$$L_{cd} = \sum_{x \in X} min_{y \in Y} \|x - y\|^2 + \sum_{y \in Y} min_{x \in X} \|y - x\|^2 \quad (1)$$

A normal distance between X and Y point clouds is used to ensure the smooth surface of the output shape. We set p as the nearest neighbor point of q in Y, then let

$$\Delta = <x, y> = \{(p, q) | \, p \in X, q \in Y\} \quad (2)$$

to represents the set of pairs $<p, q>$, and let υ_x be the observed surface normal to point x from ground truth. Then the absolute normal distance is given by

$$L_{norm} = -\left(\frac{\sum_{x,y \in \Delta} \left\|\upsilon_x \cdot \upsilon_y\right\|^2}{|X|} + \frac{\sum_{y,x \in \Delta} \left\|\upsilon_y \cdot \upsilon_x\right\|^2}{|Y|}\right) \quad (3)$$

Last, we use a Laplacian regularization defined in [1] to penalizes the unsmooth edges and vertices to guarantee the superior quality mesh predictions, which we named L_{edge} in our system. All the loss functions in our system can be concluded as:

$$L_{total} = L_{cls} + L_{box} + L_{mask} + \lambda_{cd} \cdot L_{cd} + \lambda_{norm} \cdot L_{norm} + \lambda_{edge} \cdot L_{edge} \quad (4)$$

all λ_* are to ensure the balance of all loss functions of whole system. Finally, our system combines object detection losses, instance segmentation losses and mesh prediction losses for training.

4. Experiments

4.1. Datasets

For three-dimensional shape reconstruction task, 3D-FUTURE [5] provides 5203 unique precision furniture CAD models with textures.

For evaluating our system on 3D-FUTURE, we used Blender engine to render 12 view textured renderings (with gray background) and masks for each CAD model, and then we split a validation set with 1000 clean-background images and corresponding models for measuring the quality of the predict meshes, which was called D_1. The resolution of each image is 256∗256.

Besides, 3D-FUTURE offers 11676 real interior images containing furniture objects of 2851 different models, which was named D_2. For this part, we reserve 5% of the training models and images to measure the performance of our system on real pictures.

4.2. Implementation details

To train our system on 4 Tesla M60 GPUs, we set batch-size is 8 and epoch is 50. Our system optimized using Adam with weight decay 2e-4. The learning rate is initialized as 2e-3 and warm up 3 epochs and then decays to (2e-4, 2e-5) at epoch (35, 45). Hyper parameters λ_* used in Equation (4) are $\lambda_{cd} = 1$, $\lambda_{norm} = 0.1$ and $\lambda_{edge} = 1$.

4.3. Evaluation

Following [1], we also take Chamfer Distance and Fscore as our metrics to measure the quality of the 3D shape reconstruction. Lower is better for CD, and higher is better for Fscore. To compute CD, we random sample 2048 points uniformly from the meshes surface.

4.4. Results and discussion

To validate the performance of our system in real indoor images and compare with the latest method, we trained our system and Pixel2Mesh on D_1 and D_2, respectively.

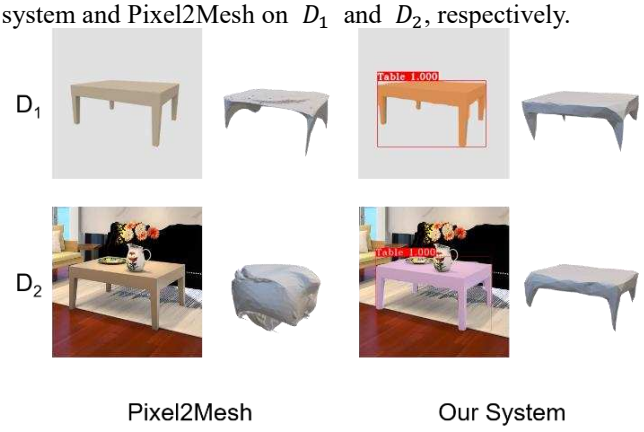


Fig.3 Comparison of results

As shown in the bottom left corner of Figure 3. Due to the interference of complex background and slight occlusion, P2M fails to find the furniture object that needs to be reconstructed. Benefit from RoIAlign proposed in [3], our system can segment and reconstructs furniture objects from real-world images correctly after adequate training.

To measure the quality of our method while compared with the latest method, we take Chamfer Distance and the harmonic mean of precision and recall (Fscore) as our metrics to measure the quality of the shape reconstruction.

The following Table 1 shows the CD and Fscore of our system and P2M on dataset D_1.

Table 1 Performance on D_1

Methods	Dataset	CD	Fscore
P2M	D_1	0.061	76.42
Ours	D_1	0.062	76.35

Due to the images of D_2 has complex backgrounds and slight occlusions, P2M can't get an effective result on D_2. The Table 2 shows the Performances of our system on dataset D_2.

Table 2 Performance on D_2

Methods	Dataset	CD	Fscore
P2M	D_2	/	/
Ours	D_2	0.079	65.87

In real indoor scenes, our system has achieved good results. The following Figure 4 shows some examples of our system's reconstruction results on real images.

Fig.4 Results on real images

5. Conclusions

In this paper, we propose an effective 3D shape reconstruction system for single-view real-world images. In contrast to most existing methods, our goal is to segment furniture objects from real indoor images, then reconstruct their 3D meshes and output their classifications, bounding boxes and masks by combining instance segmentation network MS R-CNN and 3D reconstruction network P2M. Extensive experiments have been conducted to demonstrate its effectiveness. This system can be easily applied in 3D games, AR/VR, home decoration and house rental and sale fields.

Acknowledgements

This work supported by National Key R&D Program of China (2019YFB1406202) and supported by Sichuan Science and Technology Program (2019ZDZX0009).

References

[1] N. Wang, Y. Zhang, Z. Li, Y. Fu, W. Liu, and Y u-Gang Jiang. Pixel2Mesh: 3D Mesh Model Generation Via Image Guided Deformation. In IEEE Transactions On Pattern Analysis and Machine Intelligence, 2020.

[2] H. Fan, H. Su, and L. J. Guibas. A Point Set Generation Network For 3D Object Reconstruction From A Single Image. In CVPR, 2017.

[3] X. Sun, J. Wu, X. Zhang, Z. Zhang, C. Zhang, T. Xue, J. B. Tenenbaum, and W. T. Freeman. Pix3D: Dataset And Methods For Single-Image 3D Shape Modeling. In CVPR, 2018.

[4] K. He, G. Gkioxari, P. Dollár, and R. Girshick. Mask R-CNN. In ICCV, 2017.

[5] Huan Fu, Rongfei Jia, Lin Gao, Mingming Gong, Binqiang Zhao, Steve Maybank, and Dacheng Tao. 3d-future: 3d furniture shape with texture. arXiv preprint arXiv:2009.09633, 2020.

[6] C. B. Choy, D. Xu, J. Y. Gwak, K. Chen, and S. Savarese. 3D-R2N2: A Unified Approach For Single And Multi-View 3D Object Reconstruction. In ECCV, Cham, 2016.

[7] Z. Huang, L. Huang, Y. Gong, C. Huang, and X. Wang. Mask Scoring R-CNN. In CVPR, 2020.

[8] Chang, Angel X. et al. ShapeNet: An Information-Rich 3D Model Repository. In Computer Science, 2015.

A HUMAN HEAD DETECTION METHOD BASED ON CENTER POINT ESTIMATION FOR CROWDED SCENE

LIU CHENYANG[1], GU XIAOFENG[1], KUANG PING[1], LI FAN[1], HE MINGYUN[1]

[1]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China
E-MAIL: lalchey@163.com, guxf@uestc.edu.cn

Abstract:

The head detector can effectively handle the Angle change of the head caused by motion, and the features required to capture are smaller. Therefore, human head detection is widely used in the practical application scenes of people positioning and counting. The existing head detector uses a large number of anchors which makes the detection efficiency low. And additional post-processing is required, which may result in the loss of real objects in a crowded scene. In this paper, we return to the bounding-box of the head by estimating the center point of the human head without using anchors and post-processing, which improves the detection efficiency. At the same time, we designed a random combination of data augmentation methods and improved the backbone network to improve the accuracy and robustness of the head detector in crowded scenes. Our method achieves excellent speed and precision performance on the SCUT-HEAD dataset, with 0.91 AP and 0.70 EER at 61.5 FPS.

Keywords:

Human head detection; Center point estimation; Object detection; Crowded scene;

1. Introduction

In recent years, significant research achievements have been made in the object detection area, while face detection and pedestrian detection, as two important research branches of object detection, have also made great progress. There are still some limitations in the practical application of the face detector. The face detector focuses on capturing face features and uses certain strategies to return the position and size of the face. However, in practical application scenes, the movement of the object in the camera often occurs. When the face is facing one side or the back of the camera, it is usually difficult for the face detector to catch it. In some crowded scenes, especially indoor scenes, the human body is obscured by other objects, or between human bodies is very serious. In such scenes, it is difficult to ensure high accuracy of pedestrian detection. Human head detection will not be limited by the change of head Angle. Comparing with the human body, the head object is smaller and easier to be captured by the detector in crowded scenes. Therefore, human head detection is more suitable for people positioning and counting, and performs better in specific tasks such as population statistics, density estimation, and personnel entry and exit detection.

Our detector is based on Keypoint Triplets for Object Detection [3]. Unlike the one-stage or two-stage detectors using anchors, we use the center point estimation method to detect the object. In order to better adapt to the crowded scene and improve the efficiency of the detector in industrial applications, we only estimate the center point of the head. This is different from [3] of the object's center point and two corner points. Our method proposes a data augmentation method of image random combination to obtain images with more crowded heads and enhance the robustness of the head detector. By improving the DLA network [4], the resolution of the feature map can be improved and the heatmap of the center point can be obtained in a crowded scene. According to the thermal value, the center point of the head is predicted to return the size and position information, and finally, the bounding-box is obtained. Our method had excellent speed and precision performance on the SCUT-HEAD data set, with 0.91 AP and 0.70 EER at 61.5 FPS, and achieved excellent test results in the actual scenario test.

2. Related work

Object detection. Object detection is a basic research field in computer vision and has been widely studied in the past decades. Object detection aims to find objects with a specific object class with precise positioning in a given image and assign a corresponding class label to each object

instance. As a basic technology of artificial intelligence in practical application, object detection is widely used in various fields, such as people detection. Our method is dedicated to using human head detection to quickly and efficiently complete specific tasks such as population statistics, density analysis, and personnel entry and exit detection in crowded scenes, in order to avoid the defects of face detection and pedestrian detection in practical applications.

Anchor-based methods. The anchor-based method was first proposed in the Faster R-CNN [5] and has been widely used as the main proposal generation of object detection framework in the subsequent one-stage and two-stage detectors. In this method, a large number of anchors with different sizes and aspect ratios are set in each window area of the feature map by means of sliding Windows, and thresholds are set manually to distinguish between foreground and background. Our method only predicts the center point of the human head, which is equivalent to assigning the anchor to the corresponding position without considering the size and aspect ratio. It also does not manually classify the foreground and background. Because there is no need to set up a lot of anchors, the work efficiency of our human head detector is improved in crowded scenes.

Post-processing. At present, mainstream detectors only use a large number of anchors, so they will get a large number of bounding-boxes and corresponding scores, and there are cases of bounding-boxes containing or overlapping each other. Therefore, NMS (Non-Maximum Suppression) [6] is needed as post-processing means to select those bounding-boxes with the highest scores in the neighborhood and suppress those with low scores. However, using NMS usually cannot relate the context information of the whole image, and can only infer from the attributes of the bounding-box. When object instances are crowded or overlapped, the NMS erroneously identifies two adjacent or overlapping objects as one and retains the bounding box with a higher score. This will cause the detector to fail due to false positives or missing positives. As shown in Figure 1, our method focuses only on the center point of the human head without the need for an anchor, therefore does not require the use of the NMS. The prediction of the center point is obtained from the local peaks of the heatmap, which can effectively focus on global features, thereby reducing the loss of object instances in crowded scenes and improving accuracy.

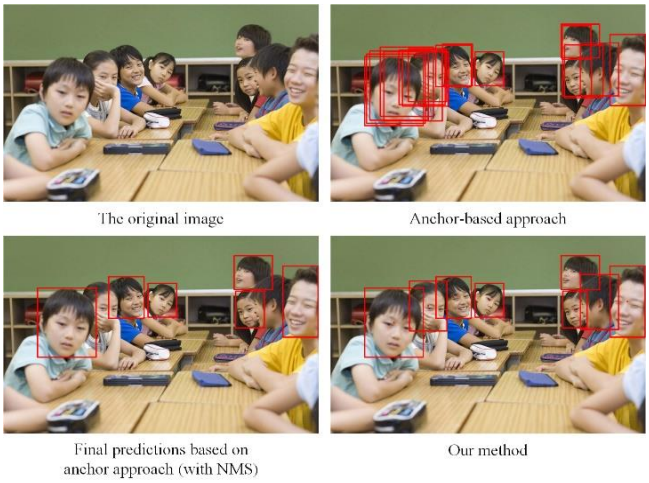


Fig.1 Original image and comparison diagram of different head detection methods

3. The proposed method

3.1. Data augmentation

We proposed a random combination data augmentation (RCDA) method to solve the problem of unbalanced sample distribution between different regions and an unbalanced head scale in a single image in the existing human head data set.

As shown in Figure 2, we randomly selected four images in the dataset for random combination, and the length and width of each image is defined as l and w, so the aspect ratio of the original input image is $r_{original} = l{:}\,w$. We set the common scaling factor $k \in (0{,}10] \cap \boldsymbol{Q}$ for the four selected images, which is random. After uniform scaling of the four images, two randomly selected images were rotated 90 degrees. The two images will be scaled equally again and their lengths combined with the width of the unrotated image to form an image in the four ways shown in Figure 2. The aspect ratio of the newly generated image can be calculated by the formula (1).

$$r_{new} = k\left(l + \frac{w^2}{l}\right){:}\,2kw \tag{1}$$

At the same time, the traditional geometric distortion augmentation methods such as symmetry and inversion are randomly adopted for each image combination, and photometric distortion augmentation methods such as image brightness, contrast, hue, and saturation are randomly adjusted. Therefore, our data augmentation method greatly increases the variability of the input image, thus making the designed head detector more robust to images in different environments and with different crowding degrees.

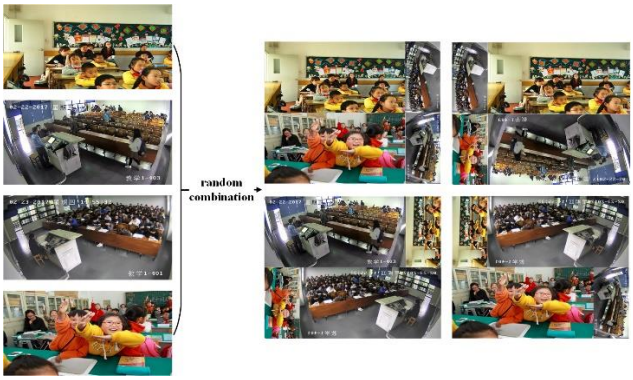


Fig.2 Random combination data augmentation method

3.2. Backbone

Our backbone network is based on DLA-34. Different from DLA-34, in order to enable the network to pay attention to more subtle details in crowded scenes, we added more skip connections and more aggregation nodes (the network structure is shown in Figure 3).

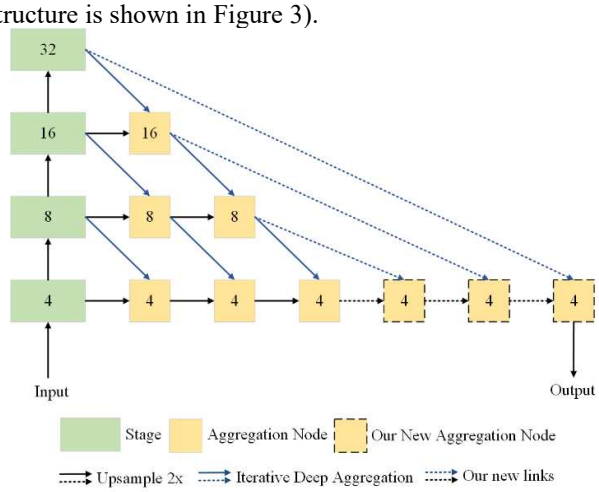


Fig.3 Improved DLA-34 network structure

Our method uses full convolutional up-sampling and hierarchical skip connections in DLA-34 networks for dense prediction. The iterative depth aggregation is used to improve the resolution of the feature map symmetrically. Specifically, we added three 3×3 aggregation nodes with 256 channels from the bottom layer and added skip connections before these aggregation nodes and the stage output heads of each resolution. A final 1×1 output convolution then produces the desired. This allows our backbone network to pay more attention to detail at all scales and make better use of layers in aggregate. The human head detector trained by our improved DLA-34 network can effectively focus on the global features and integrate the context information, thus reducing the loss of object instances in crowded scenes and improving the accuracy.

3.3. From center point to bounding-box

We used the improved DLA-34 backbone to train the center point prediction network and sampled the truth value of the head label at low resolution. Similar to [3], we also use the Gaussian kernel function (the formula is shown in formula (2)) to disperse the effective truth value and form the center point heatmap $\hat{Y} \in [0,1]^{\frac{L}{R} \times \frac{W}{R} \times C_k}$ (L and W are the length and width of the input image, R is output stride and C_k is the number of key points, in our task $C_k = 1$), but the difference is that we only focus on the center point of the object, not the corner point.

$$Y_{xyc} = \exp\left(-\frac{(x-\tilde{p}_x)^2+(y-\tilde{p}_y)^2}{2\sigma_{\tilde{p}}^2}\right) \tag{2}$$

Suppose the human head object H coordinate is $\left(x_1^{(h)},\ y_1^{(h)},\ x_2^{(h)},\ y_2^{(h)}\right)$. According to the heatmap, the local peak is taken as the predicted center point $P_h = \left(\frac{x_1^{(h)}+x_2^{(h)}}{2},\ \frac{y_1^{(h)}+y_2^{(h)}}{2}\right)$ of the human head. An offset prediction and a size prediction are designed to calculate the local offset $\hat{O}$ and size $\hat{S}$ for returning bounding-box from the center point. Therefore, two loss-functions L_o and L_s are designed based on L1 Loss respectively, where $s_h = \left(x_2^{(h)} - x_1^{(h)},\ y_2^{(h)} - y_1^{(h)}\right)$ is regression size (the loss functions are shown in formula (3)).

$$\begin{cases} L_O = \frac{1}{N}\sum_P \left|\hat{O}_{\tilde{p}} - \left(\frac{p}{R} - \tilde{p}\right)\right| \\ L_S = \frac{1}{N}\sum_{h=1}^{N}\left|\hat{s}_{p_h} - s_h\right| \end{cases} \tag{3}$$

Finally, $\hat{Y}$ is used as the degree of confidence to return the bounding-box $B\left(\hat{x}_i + \delta\hat{x}_i - \frac{\hat{l}_i}{2}, \hat{y}_i + \delta\hat{y}_i - \frac{\hat{w}_i}{2}, \hat{x}_i + \delta\hat{x}_i + \frac{\hat{l}_i}{2}, \hat{y}_i + \delta\hat{y}_i + \frac{\hat{w}_i}{2}\right)$ of the object.

4. Experiments

4.1. Dataset

Our head detector training, testing, and validation were conducted on the SCUT-HEAD dataset. SCUT-HEAD is a large-scale head detection dataset, including 4405 images labeled with 111251 heads. The dataset consists of two parts. Part A includes 2000 images sampled from monitor videos of classrooms in a university with 67321 heads annotated. Part B includes 2405 images crawled from the Internet with 43930 heads annotated. This dataset follows the standard of Pascal VOC.

4.2. Training details

During the training, we added the random combination (RCDA) method designed by us to increase the scene diversity and crowding degree of the original data set. According to the original data set, we adjusted the resolution of the original input image to 1100×550, and the aspect ratio was adjusted to $2:1$. At the same time, we set the scaling factor $k = 1$ for data aggregation, so that the aspect ratio of the processed image become $5:4$. We used two NVIDIA GTX 1080Ti for training and comparative testing. We set the epoch as 200, batch size as 4, and validated it every 20 epochs. The initial learning rate was set as 1.25e-4. Adam optimizer was used in the training process. The whole training process takes 29 hours.

4.3. Results

The detector trained using our method has an inference speed of only 0.02 seconds for head detection in a single image. We use our detector and the two current mainstream human head detectors (one is Overfeat-AlexNet [5] and the other is End-to-end [7]) to carry out a human head detection test under the same test image. Our detector loses fewer real objects in crowded scenes, has faster inference speed and higher accuracy (the comparison experimental results are shown in Figure 4).

Fig.4 Comparison of experimental results

We use AP (average precision), EER (equal error rate), and average inference speed as performance indicators, and calculate the relevant indicator data between our method and the mainstream head detectors under the SCUT-HEAD dataset. The results are shown in Table 1.

Table 1 Performance

Method	AP	ERR	Average Inference Speed
Overfeat-AlexNet [5]	0.62	0.66	4.5FPS
Overfeat-GoogleNet [5]	0.67	0.71	4.7FPS
FCHD [6]	0.70	0.77	11FPS
End-to-end [7]	0.78	0.81	21FPS
YoLov3 [8]	0.85	0.78	54FPS
Ours (without RCDA)	0.88	0.72	61FPS
Ours (with RCDA)	0.91	0.70	61.5FPS

It can be concluded from Table 1 that our method has better AP and ERR performance in a crowded scene, and has a faster inference speed.

5. Conclusions

In this paper, we propose a new human head detection method for a crowded scene based on center point estimation. The head detector trained by designing a new data aggregation method and improving the backbone network effectively reduces the loss rate of real objects and improves the speed and accuracy of human head detection. A large number of application tests have proved that our head detector can efficiently and accurately complete crowd positioning and counting tasks in crowded scenes, and is suitable for the airport, subway and other application scenes.

Acknowledgments

This work is supported by the National Key R&D Program of China (2019YFB1406202) and the Sichuan Science and Technology Program (2020GFW001, 2020YFG0320, 2018FZ0101, 2019GFW116).

References

[1] Kaiwen Duan, Song Bai, Lingxi Xie, Honggang Qi, Qingming Huang, Qi Tian, "CenterNet: Keypoint Triplets for Object Detection", Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV), 2019, pp. 6569-6578.

[2] F. Yu, D. Wang, E. Shelhamer, T. Darrell, "Deep layer aggregation", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018, pp. 2403-2412.

[3] S. Ren, K. He, R. Girshick, J. Sun, "Faster r-cnn: Towards real-time object detection with region proposal networks", In NeurIPS, 2015.

[4] A. Neubeck and L. Van Gool, "Efficient Non-Maximum Suppression", 18th International Conference on Pattern Recognition (ICPR'06), Hong Kong, 2006, pp. 850-855.

[5] Pierre Sermanet, David Eigen, Xiang Zhang, Michael Mathieu, Rob Fergus, and Yann LeCun, "Overfeat: Integrated recognition, localization and detection using convolutional networks", In ICLR, 2014.

[6] Vora, Aditya, "FCHD: A fast and accurate head detector", In CoRR, 2018.

[7] Russell Stewart, Mykhaylo Andriluka, Andrew Y. Ng, "End-to-end people detection in crowded scenes", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 2325-2333.

[8] J. Redmon and A. Farhadi, "Yolov3: An incremental improvement", arXiv preprint arXiv:1804.02767, 2018.

AN IMPROVED MULTI-SCALE FIRE DETECTION METHOD BASED ON CONVOLUTIONAL NEURAL NETWORK

HUANG HONGYU[1], KUANG PING[1], LI FAN[1], SHI HUAXIN[1]

[1]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China
E-MAIL: huanghy6268@163.com, kuangping@uestc.edu.cn

Abstract:

Fire is a major disaster in the world, and the fire detection system should accurately detect the fire in the shortest time to reduce economic loss and ecological damage. Traditional sensors are still widely used in a large number of applications, but they do not perform well in remote high-dome environments or the early stages of low-flame fires, and now the method of using image and video to predict fire is becoming more and more popular. This paper proposed an improved YOLOv4 fire detection method based on Convolutional Neural Networks (CNN). We improve the accuracy of the model through the self-built high-quality fire dataset, use the changed loss function to improve the detection ability of small-scale flames, and combine the Soft-NMS post-processing and DIoU-NMS post-processing to improve the suppression effect of the redundant Bounding box and reduce low recall rate. The experimental results of the model on our dataset show that the model has an excellent performance in fire detection and can detect multi-scale fire in real-time.

Keywords:

Fire detection; YOLOv4; DIoU-NMS; CIoU-Loss

1. Introduction

With the development of the scientific society and the dependence of human beings on fire, fires occur frequently. The spread and destructive nature of fire pose a great threat to human life and property safety. According to statistics, the forests devoured by fire around the world account for more than one percent of the world's total forest coverage and are also one of the culprits of global warming. In 2019, thousands of people died from indoor fires in China alone. These consequences all indicate the severity of fire disasters and the necessity of fire detection.

Traditional fire detection methods are widely used and mostly based on fire sensors such as temperature sensing or smoke sensing, but these methods may miss the flame in the remote high-dome environment or the early stage of fire. With the development of deep learning, fire detection methods through video surveillance platforms have begun to attract researchers' attention due to their wide detection range, fast detection speed, and little environmental interference.

Considering the strict requirement of fire detection for the real-time performance of the method, and based on the fact that YOLOv4 is one of the most excellent algorithms so far. This paper is based on the YOLOv4 and combined with the complex fire scenarios to make the following improvements:

1. We collect a large number of fire pictures and build a fire dataset containing nearly 10,000 pictures, including the open fire dataset, network fire dataset, and experimental fire dataset.

2. We improve the regression box loss function for better application in multi-scale (especially small-scale) fire detection scenarios.

3. We combine DIoU-NMS with Soft-NMS to make the model better to eliminate redundant Bounding box and reduce low recall rate.

The experimental results show that our improved YOLOv4 method can achieve 86.2% mAP (mean average precision) and 62.0 FPS (Frames Per Second). Our method has an excellent performance in fire detection and high practical application value.

2. Related Work

In recent years, fire detection methods based on video and image are usually divided into two methods:

The traditional method is based on the handwork characteristics of flame. Through the collection of color, texture, shape, and other features, the BP neural network or SVM is used for training, and the training model is used to detect the video frame. Ashraf et al. [1] proposed a smoke and fire detection method based on LBP and SVM. Dr.D.Jayashree et al. [2] proffered a method for fire detection under a monitored area based on Matlab image processing and Micro-controller unit.

The CNN and deep learning methods can easily process high-dimensional data and automatically extract features without adding other manual features. Guangyi Wang et al. [3] proposed a new forest fire detection framework based on CNN to make a dense prediction of flame area. Kun Zhou et al. [4] proposed a fire detection method that has a good performance in the complex environment.

3. Method

The core idea of YOLO is using the entire image as the input, then directly return the position of the bounding box and its category in the output layer. Compared with YOLOv1, YOLOv2 has the characteristics of "Faster, Better, Stronger", but it also has some shortcomings. YOLOv3 uses a multi-scale prediction and logistic classifier to support multi-label images and gets a better basic classification network Darknet-53 from ResNet. YOLOv4 introduces the CSP network into the backbone to build a more powerful CSPDarknet53 on the original basis, and pick an optimal framework through numerous experiments on the current object detection tricks. Yolov4 is the mainstream excellent algorithm in the industrial field today.

3.1. Architecture

In this part, we will introduce the whole architecture used.

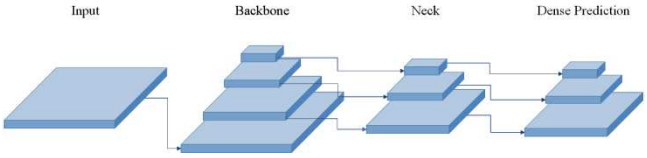


Fig.1 Object detector

We used Darknet53 network which introduces the idea of CSP as the backbone of the system as it has a higher input network size for detecting multi-scale objects and more layers to cover the ever-expanding input network and more parameters so that the model has greater ability to detect multi-objects that of different sizes just in a single image.

We added the SPP module to the backbone for it significantly increases the receptive field, isolates the most significant context features, and hardly reduces the network speed. We used PANet instead of FPN in YOLOv3 as the method of parameter aggregation, and perform parameter aggregation from different backbone layers for different detector levels.

3.2. Design of Loss Function

The loss function consists of three parts, regression box loss, confidence loss, and classification loss. When designing the regression box loss, we introduced CIoU loss and we thought that the IoU loss was similar, so we chose to introduce the λ_{IoU} parameter to add the CIoU loss branch to the basic L1 loss. Considering the uncertainty of flame labeling and the difficulty of labeling flame pictures, we hope to keep the IOU loss as low as possible within the allowable range, so we introduced the λ_{coord} and β parameters for training and debugging. We also do not want the unrecognizable part of the object, or the background part, to make up too much of the loss function, so we use the parameter λ_{noobj} as a penalty. In the process of training the model, we will optimize the following loss functions:

$$\lambda_{coord}\sum_{i=0}^{S^2}\sum_{j=0}^{B}I_{ij}^{obj}(2-w_i\times h_i)[(x_i-x_i)^2+(y_i-y_i)^2]+$$

$$\lambda_{coord}\sum_{i=0}^{S^2}\sum_{j=0}^{B}I_{ij}^{obj}(2-w_i\times h_i)[(w_i-w_i)^2+(h_i-h)^2]+$$

$$\lambda_{IoU}[1-IoU+(\frac{d^2}{c^2}+\alpha v)]^{\beta}+$$

$$\sum_{i=0}^{S^2}\sum_{j=0}^{B}I_{ij}^{obj}[C_i\log(C_i)+(1-C_i)\log(1-C_i)]+$$

$$\lambda_{noobj}\sum_{i=0}^{S^2}\sum_{j=0}^{B}I_{ij}^{noobj}[C_i\log(C_i)+(1-C_i)\log(1-C_i)]+$$

$$\sum_{i=0}^{S^2}I_i^{obj}\sum_{c\in classes}[p_i(c)\log(p_i(c))+(1-p_i(c))\log(1-p_i(c))] \quad (1)$$

The above formula that we give, I_i^{obj} means whether object appears in box i or not and I_{ij}^{obj} means that the j th bounding box predictor in box i is "responsible" for the prediction.

3.3. Non-Maximum Suppression

Since our task is a kind of object detection, our research focus is not only on whether the model can correctly classify the objects but also on the position information of the recognized objects in the whole image. We hope that the final detection results can give a more accurate description of the location of the classified objects and clearly box them for us to check. Hence the post-processing is also very significant and NMS technology is an important post-processing way in object detection to remove duplicate boxes and leave the most accurate box.

In the traditional NMS, IoU is used to eliminate the overlapping area, but in the suppression criterion, not only the overlapping area must be considered, but also the center point distance between the two boxes. Considering this

problem, we chose the distance-based IoU- Loss. DIoU NMS considers the central point to help alleviate occlusion cases and can achieve higher recall while keeping the NMS threshold unchanged.

To solve the problem of undetected error and low recall rate of Hard NMS, we introduced Soft-NMS. Soft NMS adopts a scoring penalty mechanism and uses a penalty function that is positively related to IoU to punish the scores. While the linear penalty is not smooth so we use a Gaussian penalty.

We combined DIoU NMS and Soft NMS and finally designed Soft-DIoU-NMS.

$$s_i = \begin{cases} s_i e^{-\frac{IoU(M,B_i)^2}{\sigma}}, & DIoU(M,B_i) \geq thresh \\ s_i, & DIoU(M,B_i) < thresh \end{cases} \quad (2)$$

4. Experiments

4.1. Datasets

The number of fire videos published on the Internet is small, the types of scenes are tiny, the flame scale is relatively single, and the video quality is low. So we built a high-quality fire dataset containing 10,000 fire pictures to train and test the model to improve the generalization and robustness of our model. Based on the original public fire dataset, we found many high-quality fire pictures with multi-scale on the Internet. To improve the model's performance for the recognition rate of small-scale flames and the performance in complex scenes, we also took part of the flame videos in many different experimental scenes for video interception.

We used the labelImg tool to label our self-built fire dataset. Compared with the crowd-sourced labeling fire dataset, we will try to unify labeling standards and achieve high-quality flame labeling as much as possible to improve the accuracy of our model.

Our self-built fire dataset contains a total of 10,000 fire pictures. The training set is composed of 8,400 fire pictures and the testing set is composed of 1,600 fire pictures. The fire dataset contains a variety of scenes ranging from simple to complex background, small-scale to large-scale, single object to multiple objects, indoor to outdoor environment, day and night illumination, which guarantees the good generalization ability of the improved YOLOv4 model proposed in this paper.

Fig.2 Self-built fire dataset

4.2. Training Details

In this experiment, Mosaic and Cutmix technology are used for data argument. And we also used 2 Nvidia GTX 1080Ti GPUs to train our fire detection model. We used SGD optimizer in our training and set the input to 608*608, the batch size to 128, the maximum of epochs to 60000, the learning rate to 0.001, momentum to 0.949, the weight decay rate to 0.0005. When we trained for 40,000 times, the learning rate is reduced to 0.0001; when we trained for 50,000 times, the learning rate is further reset to 0.00001. The whole training process took about four days.

Fig.3 Mosaic for data augmentation

4.3. Results

To verify the fire detection effect of our method for the detection of multi-scale (especially small-scale) flames in different complex scenes, we tested our trained fire detection model on multiple actual and experimental fire videos, and the self-built fire detection dataset was based on the flame scale to account for the proportion of the image. It is divided into small-scale, medium-scale, large-scale, and extra-large-scale flame samples. Some of the prediction results are shown below.

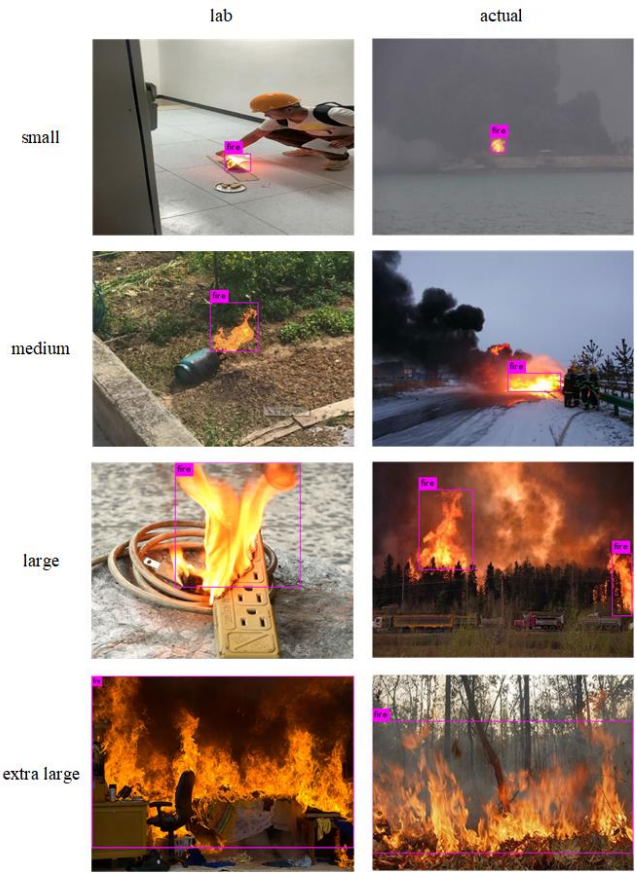


Fig.4 Prediction results of actual and lab test fire videos

4.4. Test and Verify

To further verify the specific performance of our method in fire detection, the method we proposed and other mainstream object detection methods such as SSD, YOLOv3, YOLOv4 are compared and analyzed on the same fire dataset. The performance test results of four methods as shown below.

Table 1 Performance comparison

Method	mAP	FPS
SSD	0.76	45
YOLOv3	0.81	50
YOLOv4	0.84	55
Our Method	**0.862**	**62**

As we can see from the table, our method achieves the best results in both accepted metrics.

5. Conclusion

This paper proposed a new network architecture based on the YOLOv4 and designed the fire detection model based on the Darknet deep learning framework. In the experiment, we used a large number of self-built fire dataset including multi-scale for training and testing. The results showed that our model has a better performance in fire detection.

Acknowledgements

This work supported by Sichuan Science and Technology Program (2020YFG0309、2019ZDZX0005、2020GFW001).

References

[1] Russo A U, Deb K, Tista S C, et al. “Smoke Detection Method Based on LBP and SVM from Surveillance Camera”, 2018 International conference on computer, communication, chemical, material and electronic engineering, pp. 1–4, 2018.

[2] Jayashree D, Pavithra S, Vaishali G, et al. “System to Detect Fire under Surveillanced Area”, 3rd IEEE International Conference on Science Technology Engineering and Management, pp. 214-219, 2017.

[3] Wang G, Zhang Y, Qu Y, et al. “Early Forest Fire Region Segmentation Based on Deep Learning”, Chinese Control And Decision Conference, pp. 6237-6241, 2019.

[4] Zhou K, Zhang X. “Design of Outdoor Fire Intelligent Alarm System Based on Image Recognition”, International Journal of Pattern Recognition and Artificial Intelligence, Vol. 34, No. 07, 2019.

AN IMPROVED KUBERNETES SCHEDULING ALGORITHM FOR DEEP LEARNING PLATFORM

SHI HUAXIN[1], GU XIAOFENG[1], KUANG PING[1], HUANG HONGYU[1]

[1]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China
E-MAIL: shi_huaxin@163.com, guxf@uestc.edu.cn

Abstract:

Most existing deep learning platforms only focus on helping users to start task training quickly, but they tend to ignore the application scenario of multi-team collaboration using one resource pool. In this paper, we propose an improved scheduling algorithm oriented to a multi-tenant model, in which team users are modeled as virtual clusters and cluster load will be monitored regularly. We apply the optimized Kubernetes scheduling algorithm to the Docker-based deep learning platform, our method can ensure the load balance and meet the needs of users.

Keywords:

Kubernetes; Docker; Deep Learning

1. Introduction

The development of deep learning has brought new solutions to traditional problems in the computer field. As a hot topic in academia and a new opportunity in the industry, it has received high attention and extensive support. As an infrastructure for performing algorithm training and optimizing network models, building a deep learning platform for data processing and model training has important significance.

The traditional methods of deep learning training are individuals or organizations purchasing hardware facilities, configuring the corresponding deep learning environment on a computer or server, and directly performing training in the completed environment. This series of steps has a high threshold in terms of economy and experience, and it is difficult to promote to all walks of life. It provides many obstacles for the public to carry out deep learning research and development. For colleges and universities, laboratory teams are often equipped with server clusters of a certain size, but students need to manually carry out environment configuration work by themselves, which is not only difficult to get started but also easily affects the experimental environment of others.

In recent years, major cloud service providers have begun to develop and launch deep learning platforms gradually. Google cloud platform [1] can provide users with deep learning cloud server trial applications. Baidu Paddle Paddle [2] provides users with a deep learning one-stop platform, including AI model customization services, AI training tutorials, and model training deployment. Tencent uses Java and Scala development With Angel [3], a model training platform for machine learning and graph computing. FloydHub [4] provides users with mainstream data sets and deep learning frameworks to facilitate users to conduct model training as soon as possible. Most of the existing deep learning platforms can bring convenience to users in training, but they have poor adaptability to the application scenario of multi-team collaborative development in university laboratories.

In this paper, we propose an improved multi-tenant model-oriented Kubernetes scheduling algorithm. Based on the HiveDScheduler scheduling strategy that models users as virtual clusters, we measure the load situation of the cluster periodically, the pod on the node is scheduled to make the cluster load balancing. Our method improves the stability and availability of the platform, and perform well in multi-team collaborative development scenarios.

2. Related works

2.1. Virtualization

The mainstream virtualization technologies include platform virtualization technology and operating system-level virtualization technology.

The typical representative of platform virtualization technology is KVM [5]. The principle is to provide users with a unified management abstract computing environment by setting up control programs on actual physical machines. The operating system running on the actual physical machine is called Host OS, and the computing environment provided

to users is called a virtual machine.

The operating system-level virtualization technology is implemented by the Host OS kernel directly. The original system kernel is virtualized and an independent abstract computing environment is divided, so that different computing environment can share the underlying hardware resources. The computing environment generated by operating system-level virtualization technology is also called a container, and its typical representative is LXC [6].

The comparison of the architecture of the two virtualization technologies is shown in Fig.1. The virtualization technology based on the container occupies fewer resources and has better portability.

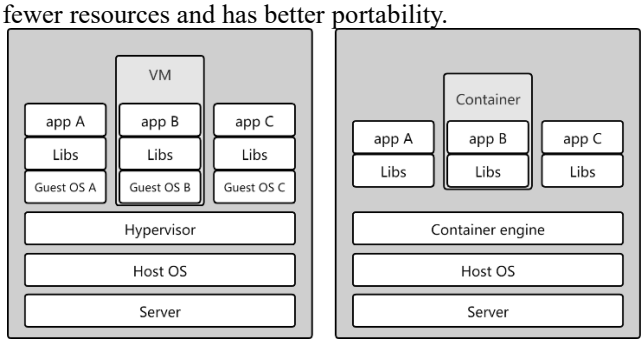


Fig.1 Structure of VM and Container

2.2. Docker

Docker [7] uses API to expand and further package based on Linux Container to make user operations easier, it uses Cgroups and Namespace to complete core virtualization operations. The Namespace mechanism provides different namespaces for processes. This mechanism implements the isolation of container technology permissions by placing different processes in isolated containers to run. The Cgroups mechanism forms a hierarchical control group through hierarchical division and process control, sets upper and lower limits for the resources that can be used by the container, and realizes the isolation of the container technology on resources.

Docker uses Union File System as the basis of the image. Union FS is a hierarchical file system that can modify files by creating and overlaying layers. The Docker hierarchy is shown in Fig.2. The image is a static file system obtained by overlaying multiple read-only layers. The container is a dynamic process that adds a read-write layer to the image. Different containers can share the same read-only mirroring layer, so they will not reuse resources. When users use docker technology, the docker will add a new layer that can be read and written on top of the original layer and generate a container. All modification operations will be written to the top layer without affecting the bottom layer image.

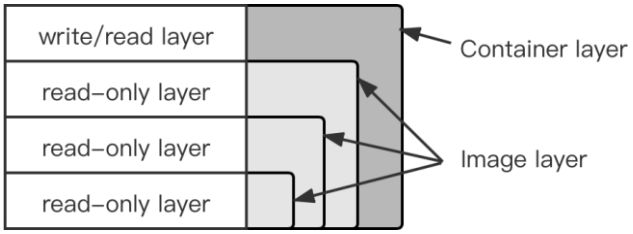


Fig.2 Docker hierarchy

2.3. Kubernetes

Kubernetes [8] is an open-source container orchestration engine optimized based on the container management systems Borg and Omega used by Google internally. The purpose of its development is to design a mechanism for configuring, deploying, managing, and maintaining containers to make the deployment of containerized applications easier and more efficient. Now, Kubernetes has been widely used in the public cloud, private cloud, hybrid cloud, and other scenarios due to its good portability and scalability.

Kubernetes is often used for cluster management to deploy containerized applications. It sets the nodes in the cluster as two identities: Master and Worker. Master is the central node that performs control and management operations in the entire cluster, and Worker is the working node in the cluster that maintains Pod and provides the component operating environment.

The Master includes the following components:

a) ETCD: It is used to store data in the Kubernetes cluster and is the default backend database.

b) Kube API server: As an API server in the cluster, it provides an interface for resource request/call.

c) Kube Controller manager: As the control manager in the cluster, it compiles the background processes in the cluster into binary files to manage processes and services.

d) Kube Scheduler: Regards pods as the basic unit of cluster scheduling to ensure that newly created pods can be allocated to nodes in the cluster.

The Worker includes the following components:

a) Pod: As the basic unit of scheduling in the cluster, it guarantees the scalability and scalability of the cluster. One or more containers will be placed in the pod to form an application and run. The Kubernetes cluster monitors the pod to ensure the normal operation of the container.

b) Kubelet: As the main agent and communication engine of the nodes in the cluster, it monitors the running status and health check of the containers in the pod on the node.

c) Kube proxy: Maintain network rules in the cluster and ensure the availability of container services running in

the cluster.

The Structure of Kubernetes is shown in Figure 3.

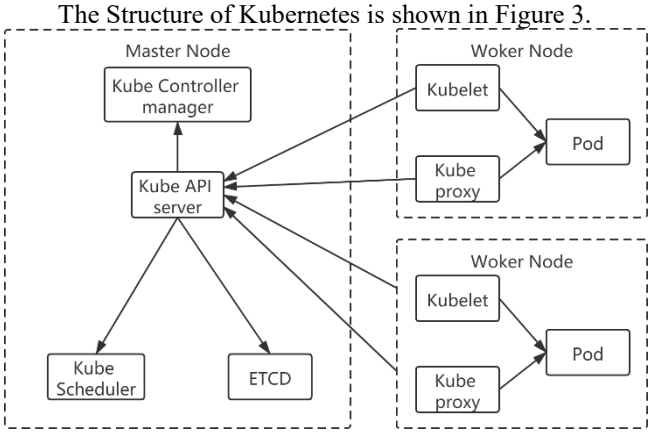


Fig.3 Structure of Kubernetes

3. Design and implementation

3.1. Docker-based platform construction

We built the platform based on Microsoft's open-source platform OpenPAI. The components needed to build the platform were packaged in the Docker image and uploaded to the Docker hub. In the process of deploying the platform, image files are pulled according to the scale of the cluster and distributed to nodes. Docker hub provides version control of image files, which makes it easy to modify and replace the components of the platform. The components in the system are lightweight and reusable. The entire platform is composed of a modular structure.

We configure the deep learning environment according to the hardware conditions of the nodes in the cluster and upload it to the Docker hub. When using the platform for deep learning training, users can directly select the configured environment, the cluster selects the appropriate node according to the scheduling algorithm and pulls the docker image.

3.2. Kubernetes scheduling algorithm optimization

This paper designs an improved Kubernetes scheduling algorithm, based on the combination of the improved HiveDScheduler scheduling strategy and the default Kube-scheduler. Our method can meet the needs of users while ensuring cluster load balancing.

HiveDScheduler. On the premise that users of multiple teams use the same resource pool, HiveDScheduler puts forward the concept of virtual clusters, which models different users into different virtual clusters, and sets fixed computing resources for each virtual cluster. For a single virtual cluster, users within the cluster have the highest priority and can use the allocated resources at will. When a virtual cluster has a high degree of idleness, users outside the cluster can also use the computing resources in the cluster for work, but their priority is lower. This design can meet the needs of users from multiple teams to share the same resource pool while improving resource utilization.

The default Kube-scheduler. Kube-scheduler includes two steps: filtering and scoring. In the filtering step, the filter checks whether a node meets the requirements for resource requests of a pod, and gets the set of available nodes to schedule the pod. In the filtering step, the scheduler chooses the optimal node by ranking the set of available nodes. The scheduler can find nodes with more remaining resources and fewer existing pods.

The optimization algorithm we proposed has made some modifications. In the scoring steps, we use the CPU occupancy rate, GPU occupancy rate and memory utilization rate of the nodes in the cluster to calculate and measure the busyness of nodes.

Define the number of CPU cores of the node i as C_{cpu}, the number of GPU cores as C_{gpu}, the CPU frequency as $Score(cpu_i)$, the GPU frequency as $Score(gpu_i)$, and the memory size as $Score(memory_i)$, whose weights are λ_{cpu}, λ_{gpu} and λ_{memory} respectively, where:

$$\lambda_{cpu} + \lambda_{gpu} + \lambda_{memory} = 1 \quad (1)$$

The performance score of the node i is $Score(p_i)$:

$$Score(p_i) = \lambda_{cpu} \times C_{cpu} \times Score(cpu_i) + \lambda_{gpu} \times C_{gpu} \times Score(gpu_i) + \lambda_{memory} \times Score(memory_i) \quad (2)$$

Define the CPU utilization rate of the node i as $U(cpu_i)$, GPU utilization rate as $U(gpu_i)$, memory utilization rate as $U(memory_i)$, and total load as $Load(n_i)$:

$$Load(n_i) = \lambda_{cpu} \times U(cpu_i) + \lambda_{gpu} \times U(gpu_i) + \lambda_{memory} \times U(memory_i) \quad (3)$$

Define the total score of the node as $Score_i$, the busier the node, the lower the score, the more idle the node, the higher the score:

$$Score_i = 10 - \left\lfloor 10 \times \frac{Load(n_i)}{Score(p_i)} \right\rfloor \quad (4)$$

By calculating the average score of nodes, nodes with a lower score than the average are obtained and marked as busy nodes. The scheduler periodically checks the node load through a timer and does not schedule the POD to the busy node.

The improved scheduling algorithm flow for the multi-tenant model that we finally obtained:

Step 1: Set up virtual clusters in the Kubernetes cluster configuration according to the needs of different teams, and set the required hardware resources for a single cluster.

Step 2: Set the weight factor of the node scoring and the timer monitoring period according to the usage requirements.

Step 3: Check the load of each node in the cluster according to the cycle time set by the timer periodically.

Step 4: Calculate the scores of nodes in the cluster according to the collected load conditions, and mark busy nodes according to the average scores.

Step 5: On the premise of ensuring the isolation of the virtual cluster, schedule pod to unmarked nodes as much as possible until the cluster reaches load balancing. When the cluster enters a new load, return to the second step.

4. Result

We use a cluster with 3 nodes to test. Each node is equipped with 4 Nvidia Tesla M60 GPU. The nodes are named master, node01, and node02. The software configuration selected in the platform is shown in Table 1.

Table 1 Software configuration

Host OS	Ubuntu 16.04
Nvidia Driver	430.64
Docker	19.03.12
Kubernetes	1.15.11
OpenPAI	1.0.1
Grafana	4.6.3

We create two virtual clusters named cluster01 and cluster 02, bound cluster01 to master and node1, bound cluster02 to node2, assign 4 GPUs to each cluster. We submit two cifar10 classification tasks written by Pytorch to each virtual cluster. The CPU usage and GPU usage in the cluster are shown in Fig.4.

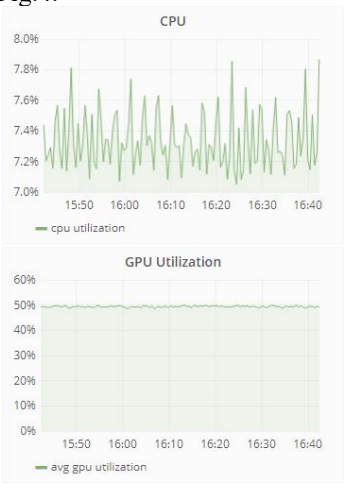


Fig.4 Cluster usage

5. Conclusion

This paper presents an improved Kubernetes scheduling algorithm for a multi-tenant model. The experiment shows our method can meet the needs of users of different teams, and detect the load of the cluster to ensure load balance periodically.

Acknowledgements

This work supported by Sichuan Science and Technology Program (2019ZDZX0005、2019ZDZX0009).

References

[1] Shah J, Dubaria D, “Building modern clouds: using docker, kubernetes & Google cloud platform”, 2019 IEEE 9th Annual Computing and Communication Workshop and Conference, pp. 0184-0189, 2019.

[2] Ma Y, Yu D, Wu T, et al, “PaddlePaddle: An open-source deep learning platform from industrial practice”, Frontiers of Data and Domputing, Vol 1, No. 1, pp. 109-119, 2019.

[3] Jiang J, Yu L, Jiang J, et al, “Angel: a new large-scale machine learning system”, National Science Review, Vol 5, No. 2, pp. 216-236, 2018.

[4] https://floydhub.com/

[5] Habib I, “Virtualization with KVM”, Linux Journal, Vol 2008, No. 166, pp. 8, 2008.

[6] Bernstein D, “Containers and cloud: From lxc to docker to kubernetes”, IEEE Cloud Computing, Vol 1, No. 3, pp. 81-84, 2014.

[7] Merkel D, “Docker: lightweight linux containers for consistent development and deployment”, Linux journal, Vol 2014, No. 239, pp. 76-90, 2014.

[8] Burns B, Grant B, Oppenheimer D, et al, “Borg, Omega, and Kubernetes”, Communications of the ACM, Vol 59, No. 5, pp. 50-57, 2016.

COMPARATIVE ANALYSES OF BERT, ROBERTA, DISTILBERT, AND XLNET FOR TEXT-BASED EMOTION RECOGNITION

ACHEAMPONG FRANCISCA ADOMA[1], NUNOO-MENSAH HENRY[2], WENYU CHEN[1]

[1]Computational Intelligence Lab, School of Computer Science and Technology, University of Electronic Science and Technology of China, Chengdu, China
[2]Connected Devices Lab, Department of Computer Engineering, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana
E-MAIL: francaadoma@gmail.com, hnunoo-mensah@knust.edu.gh, cwy@uestc.edu.cn

Abstract:

Transformers' feat is attributed to its better language understanding abilities to achieve state-of-the-art results in medicine, education, and other major NLP tasks. This paper analyzes the efficacy of BERT, RoBERTa, DistilBERT, and XLNet pre-trained transformer models in recognizing emotions from texts. The paper undertakes this by analyzing each candidate model's output compared with the remaining candidate models. The implemented models are fine-tuned on the ISEAR data to distinguish emotions into anger, disgust, sadness, fear, joy, shame, and guilt. Using the same hyperparameters, the recorded model accuracies in decreasing order are 0.7431, 0.7299, 0.7009, 0.6693 for RoBERTa, XLNet, BERT, and DistilBERT, respectively.

Keywords:

Natural Language Processing; Transfer Learning; Emotion Detection; BERT; DistilBERT; RoBERTa; XLNet

1. Introduction

The advent of social media and its gains have led to exponential increases in social media users. The number of active social media users, notwithstanding the global effect of the COVID-19 pandemic, has increased by over a hundred million representing a growth of more than 10 percent from the previous year-2019. Harnessing these social media users' profiles for polarity assignment serve as a bedrock for sentiment analysis (SA). However, the coarse granular attribute of SA in representing user profiling makes it ineffective. A subtler granular method has been shown to portray users' detailed view and thus more suited for user profiling. The detection or recognition of emotions happens to be an extraction of finer-grained user sentiments. Text-based emotion recognition is a sub-branch of emotion recognition (ER) that focuses on extracting fine-grained emotions from texts. Though research in the field is fast gaining traction, the challenge of identifying appropriate embedding techniques for extracting the relationship between long term dependent texts and parallel processing of text sequence has for long inhibited the pace of attaining state-of-the-art results. The proposal of transformers [1] and the transformer language model [2] provided a breakthrough in solving these limitations.

The Bidirectional Encoder Representations from Transformers (BERT) pre-trained model [3], using the vanilla transformer language model [2] released by Google in 2018 as a substructure, has been described as the rediscovery to the Natural Language Processing (NLP) pipeline due to the improved level of language understanding it offers [4]. However, the BERT model suffers from fixed input length size limitations, wordpiece embedding problems, and computational complexities [5]. The Generalized Auto-regression Pre-training for Language Understanding (XLNet), Robustly optimized BERT pre-training Approach (RoBERTa), and DistilBERT pre-trained models were necessary proposals for mitigating different underpinning problems associated with BERT. While BERT and its variants are being used actively in question answering (QA), natural language inference (NLI), text summarization (TS), and other NLP tasks to solve human-related and environmental problems, little has been seen in recognizing emotions from texts.

This paper aims to shed light on the efficacy of the BERT, RoBERTa, DistilBERT, and XLNet models in recognizing emotions from the International Survey on Emotion Antecedents and Reactions (ISEAR) dataset [6]. The experiments and results obtained from the four models are comparatively discussed concerning their accuracy, precision, and recall on the ISEAR dataset's emotion classes. It is worth stating that no work has comparatively analyzed the efficacy of BERT, RoBERTa, DistilBERT, and XLNet on the ISEAR dataset to the best of our knowledge.

The organization of the paper is as follows; Section 2

discusses related works; Section 3 highlights the emotion detection pipeline and model implementation. The model experiments are outlined in Section 4. The results obtained are presented and discussed in Section 5. In Section 6, the conclusion and future works are highlighted

2. Related Work

Alotaibi [7] proposed a supervised logistic regression approach to detect emotions from texts. The data they obtained from ISEAR was divided for training and testing. In the training process, sentences carrying emotions were fed into their logistic regression model and their emotion labels. Only the unseen emotion labeled sentences were passed through the trained classifier for prediction in their testing process. They evaluated their model's performance using precision, recall, and F1-score. They reported an F1-score of 0.76, 0.64, 0.73, 0.62, and 0.57 for joy, fear, sadness, shame, and guilt emotion classes. They hinted that a deep learning model could perform better on engineering the features for classification.

In response to Alotaibi's recommendation, Polignano *et al*. [8] designed a model that implemented Bi-LSTM, Self-Attention, and Convolutional Neural Networks (CNN) together. They focused on the extraction of word embeddings as a fundamental feature to improving the recognition of emotions from texts. Thus, they compared the Google word embedding performance, the GloVe embedding, and the Fast-Text embedding using the Bi-LSTM, Convolutional Neural Network (CNN) ensemble, and a Self Attention model. They evaluated their model on the ISEAR dataset, the SemEval-2018 Task 1 dataset, and the SemEval-2019 Task 3 dataset. They reported improved performance on all the datasets with the FastText embedding. They, therefore, recommended that a robust pre-trained word embedding could enhance the model performance.

Kazameini *et al*. [9] extracted contextualized word embeddings from text data using the BERT pre-trained model and used the bagged-SVM classifier to predict the authors' personality traits automatically. The input to their model was essays. The essays were divided into sub-documents, preprocessed, and fed into a BERT base model. Feature vectors for the document were extracted and fed into ten SVM classifiers to produce a prediction. The final prediction was obtained by majority voting. They obtained an increased performance of 1.04% in comparison with baseline methods.

3. Methodology

This section elucidates the various blocks of the machine learning pipeline used for the detection task, as illustrated in Figure 1. The dataset was acquired, preprocessed, and fed to the various candidate models. The candidate models were all fine-tuned on the data before final predictions were carried out.

3.1. Data Acquisition

The ISEAR dataset [10] is a publicly available dataset constructed through cross-culture questionnaire studies in 37 countries. It contains 7666 sentences classified into seven distinct emotion labels: joy, anger, sadness, shame, guilt, surprise, and fear. Its balanced class feature makes it ideal for making generalized predictive inferences; hence, its use for this study. Table 1 presents the data distribution of the ISEAR dataset.

Fig.1 The Machine Learning pipeline for the detection task

Table 1 Data Distribution of the ISEAR Dataset

Emotion Labels	Quantity
Anger	1096
Disgust	1096
Sadness	1096
Shame	1096
Fear	1095
Joy	1094
Guilt	1093
Total	7666

3.2. Data Preprocessing

The obtained data contained several columns; the columns containing individuals' responses and the emotion labels were the columns of interest to this work. These two columns were, therefore, extracted for further processing. It was also realized that some columns contained emotion labels but no textual responses. These were again removed and the total amount of data reduced from 7666 to 7589. Special characters, double spacing, tags, and other irregular expressions found in the remaining data were removed. They were noticed to affect recognition performance negatively. Stop words were further removed, and the seven emotion labels encoded to a numerical scale (i.e., 0, 1, 2, 3, 4, 5, 6). All the above preprocessing schemes were carried out before the final data samples were split into two groups, i.e., 80% for training and 20% for testing purposes. Investigations revealed that the longest sentence in the dataset had 178

words; this helped set the maximum sentence length of 200 for the tokenizer. The decision was to ensure that no sentence was truncated, and all sentences had the same length. As a result, all sentences were padded to attain a length of 200. The training and test samples were tokenized to generate the tokens, which were then fed to the fine-tuning candidate models.

3.3. Model Fine-Tuning and Classification

The generated tokens were converted to vector representations and fed to the pre-trained models during the fine-tuning process. Thus, the models were trained on the input vector transformations and their outputs generated. The output was then evaluated using the designated test data, and results were obtained. Emotions were then classified into joy, sadness, fear, anger, guilt, disgust, and shame for each of the pre-trained models in the emotion classification process.

4. Model Experiments

Experiments were carried out using Google Colab's GPU hardware accelerator platform. The extracted features for the training set were fed to the input of the tuned models. The batch size and learning rate were set to 16 and $4*10^{-5}$, respectively. The models were optimized using the Adam optimizer, and the loss parameter was set to *sparse_categorical_crossentropy*. The models were trained for ten epochs.

The BERT-base-uncased model consisting of twelve layered transformer blocks with each block containing twelve head self-attention layers and 768 hidden layers resulting in approximately 110 million parameters, was used. A single sentence was fed into the model at a time. The input sentences were split into tokens and mapped to their indexes using the BERT tokenizer library, indicated as *input_ids*. The [CLS] (classification token) and [SEP] (separate segment token) were appended at the beginning and end of every sentence, respectively. An input attention mask of fixed length with 0 indicating padded tokens, and 1, indicating unpadded tokens was applied. Each of the transformers indicated received a list of token embeddings and produced a feature vector of the same length at the output. The output of [CLS] for the 12*th* transformer layer containing vector transformations of prediction probabilities was used as aggregated sequence representation from which classifications were made.

The RoBERTa-base model was made up of twelve transformer layers with 768-hidden layers, twelve attention heads, and 125 million parameters used in the experiment. The RoBERTa tokenizer was used to encode the input texts into tokens and designated them as the *input_ids.* These ids were padded to a fixed length to avoid variations per row. Features were then extracted from these tokens from which sentence pair classification was made.

The DistilBERT-uncased model was used in this experiment. It contained six transformer layers, 768-hidden layers, and twelve attention heads. After tokenizing the input texts and converting the tokens into *input_ids*, they were padded and fed into the DistilBERT model for the multiclassification task.

The XLNet-base-cased model was made up of twelve transformer layers with 768 hidden layers. Twelve attention head layers were used. The XLNet tokenizer was used to split the sequences into tokens. The tokens were then padded, and classifications were made.

5. Results and Discussion

This section discusses in detail the results obtained for the individual models. The time taken for each model to run to completion, model accuracy, performance in detecting the seven emotion labels, and the revealed difficulties are elucidated.

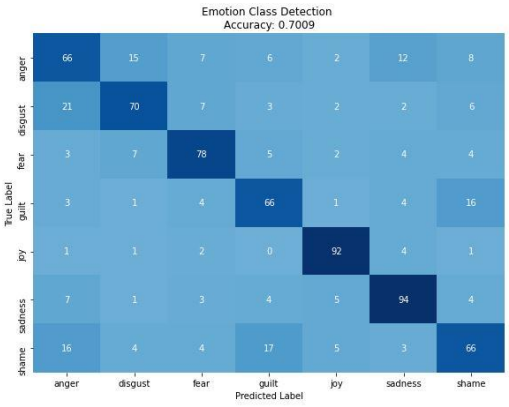


Fig.2 Confusion Matrix for BERT

The confusion matrices attained after the experiments are presented as Fig.2, Fig.3, Fig.4, and Fig.5 for BERT, RoBERTa, DistilBERT, and XLNet. The classification report presented in Table 2 indicates the various precision, recalls, and F1-scores for the individual emotion classes after testing the various candidate models on the test data.

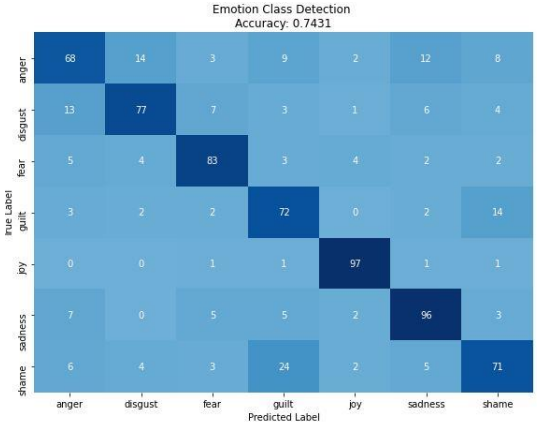


Fig.3 Confusion Matrix for RoBERTa

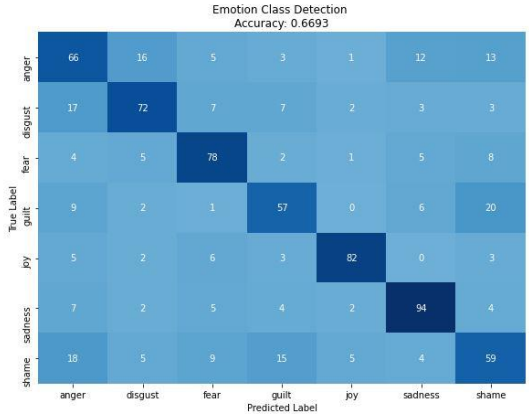


Fig.4 Confusion Matrix for DistilBERT

Fig.5 Confusion Matrix for XLNET

As shown in the confusion matrices, the order of emotion recognition accuracy in decreasing order are RoBERTa, XLNet, BERT, and DistilBERT, with a recognition accuracy of 0.7431, 0.7299, 0.7009, and 0.6693, respectively. Since all models were capable of recognizing emotions from the data, we posit that not only are these models efficient in other NLP tasks but are also efficient in recognizing emotions from texts. Secondly, from the results, we posit that under the same conditions, the RoBERTa pre-trained model outperforms the other pre-trained models under investigation in this work. Observations made during this work showed that even though the DistilBERT yielded the least accurate results, it was the fastest computationally. The XLNet model, on the other hand, was computationally the slowest. RoBERTa slightly outperformed the BERT model in speed. The order of computational resource demand in decreasing order can be given as XLNet, BERT, RoBERTa, DistilBERT. It is worth mentioning that the pre-trained models under discussion in this paper were all fine-tuned on the ISEAR dataset to obtain results. It makes us believe that the RoBERTa pre-trained model can be highly effective in recognizing emotions from texts when thoroughly optimized for the purpose. The classification report presented in Table 2 clearly shows that RoBERTa responded well to most emotion classes. The report further buttresses that RoBERTa is an optimal candidate for detecting emotions on the ISEAR dataset. XLNet also demonstrated some level of efficacy in some aspects of the seven classes. DistilBERT and BERT, on the other hand, could not achieve any high scores in any of the seven emotion classes for the precision, recall, and F1-score. The lower computational complexity of RoBERTa over XLNet also reinforces the recommendation of RoBERTa for emotion recognition in text.

6. Conclusion and Future Work

In conclusion, the paper set out to assess the efficacy of the BERT, RoBERTa, DistilBERT, and XLNet pre-trained transformer models in recognizing emotions from the ISEAR dataset. The models proved efficient in detecting emotions from the text, with RoBERTa attaining the highest recognition accuracy. The precision, recall, and F1-scores further proved the efficacy of RoBERTa over the other candidate models in recognizing emotions on the ISEAR dataset. In the future, an ensemble of the model would be considered to improve recognition performance. Also, strategies to inculcate commonsense knowledge into the model would be considered to improve its generalization ability.

Table 2 Comparison of Precision, Recall And F1-scores of BERT, RoBERTa, DistilBERT, and XLNET on the ISEAR Dataset

Models	Anger			Disgust			Fear			Guilt			Joy			Sadness			Shame		
	P	R	F1	P	R	F1	P	R	F1	P	R	F1	P	R	F1	P	R	F1	P	R	F1
BERT	0.56	0.57	0.57	0.71	0.63	0.67	0.74	0.76	0.75	0.65	0.69	0.67	0.84	0.91	0.88	0.76	0.8	0.78	0.63	0.57	0.6
RoBERTa	**0.67**	**0.59**	**0.62**	**0.76**	0.69	**0.73**	**0.8**	**0.81**	**0.8**	0.62	**0.76**	0.68	0.9	**0.96**	**0.93**	**0.77**	**0.81**	**0.79**	**0.69**	**0.62**	**0.65**
DistilBERT	0.52	0.57	0.55	0.69	0.65	0.67	0.7	0.76	0.73	0.63	0.6	0.61	0.88	0.81	0.85	0.76	0.8	0.78	0.54	0.51	0.52
XLNET	0.59	0.57	0.58	0.69	**0.73**	0.71	0.76	**0.81**	0.78	**0.7**	0.72	**0.71**	**0.91**	0.93	0.92	0.76	**0.81**	**0.79**	**0.69**	0.57	0.63

References

[1] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin, "Attention is all you need," in Advances in neural information processing systems, pp. 5998–6008, 2017.

[2] R. Al-Rfou, D. Choe, N. Constant, M. Guo, and L. Jones, "Character-level language modeling with deeper self-attention," in Proceedings of the AAAI Conference on Artificial Intelligence, vol. 33, pp. 3159–3166, 2019.

[3] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "Bert: Pre-training of deep bidirectional transformers for language understanding," arXiv preprint arXiv:1810.04805, 2018.

[4] I. Tenney, D. Das, and E. Pavlick, "Bert rediscovers the classical NLP pipeline," arXiv preprint arXiv:1905.05950, 2019.

[5] F. A. Acheampong, C. Wenyu, and H. Nunoo-Mensah, "Text-based emotion detection: Advances, challenges, and opportunities," Engineering Reports, vol. 2, no. 6, pp. 1–24, 2020.

[6] K. R. Scherer and H. G. Wallbott, "Evidence for universality and cultural variation of differential emotion response patterning.," Journal of personality and social psychology, vol. 66, no. 2, p. 310, 1994.

[7] F. M. Alotaibi, "Classifying text-based emotions using logistic regression," VAWKUM Transactions on Computer Sciences, vol. 16, no. 2, pp. 31–37, 2019.

[8] M. Polignano, P. Basile, M. de Gemmis, and G. Semeraro, "A comparison of word-embeddings in emotion detection from text using BiLSTM, CNN and self-attention," in Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization, pp. 63–68, 2019.

[9] A. Kazameini, S. Fatehi, Y. Mehta, S. Eetemadi, and E. Cambria, "Personality trait detection using bagged SVM over BERT word embedding ensembles," 2020.

[10] K. Scherer and H. Wallbott, "International survey on emotion antecedents and reactions (ISEAR) (1990)," 2017

3D RECONSTRUCTION BASED ON GAT FROM A SINGLE IMAGE

YANG DONGSHENG[1], KUANG PING[1], GU XIAOFENG[1],

[1]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China
E-MAIL: dongsheng.77@foxmail.com，kuangping@uestc.edu.cn，guxf@uestc.edu.cn

Abstract:

Previous methods which generate 3D shape usually use volume or a point cloud. These 3D shapes would lose details and are not smooth on the surface. This paper aims to introduce an end-to-end deep learning architecture which can generate 3D shape in triangular mesh from a single image. The architecture uses the graph attention network to continuously deform the initial ellipsoid based on the features extracted from a single image. The deformation process is constantly refined. The method can produce high precision mesh mode with richer details.

Keywords:

Graph attention neural network; 3D shape generation; Mesh reconstruction

1. Introduction

3D reconstruction technology is a core direction of computer vision. The existing representations can be roughly divided into four categories: depth map; voxel-based representations [2], point-based representations [3], and mesh representation [1]. The depth map is a 2D picture expressed in grayscale. Each pixel records the distance from the viewpoint to the object. The 3D reconstruction algorithm based on the depth map is not yet available, because it is more used to visualize specific 3D information in 2D pictures than to process data. The concept of volume pixels is similar to the definition of pixels in 2D. Like pixels, voxels (Fig.1(b)) do not contain position coordinates in space. Point cloud (Fig.1(a)) uses points that record coordinates information to represent 3D objects. However, the representation based on voxels and point clouds has lost important surface details, and the surface model cannot be reconstructed well. The mesh representation (Fig.1(c)) method has the characteristics of lightweight and rich shape details. It is important to have connections between adjacent points.

For the representation and processing of the network, we use graph attention neural network [4]. The structure of the graph is generally very irregular and can be considered as infinite-dimensional data. So it has no translation invariance, which makes both conventional feature extraction network invalid. The mesh describes 3D objects by vertices, edges, and faces, which exactly corresponds to the graph neural network.

Fig.1 It can be seen that the 3D reconstruction based on point cloud and voxel has lost many details. 3D reconstruction based mesh has higher quality and better details.

In this paper, we base on the architecture of Pixel2Mesh [1] which uses GCN to represent 3D objects. Pixel2Mesh extracts feature from pictures and then merges them with three-dimensional features to continuously refine the deformation. We introduce an attention mechanism in the graph algorithm to improve GCN used by Pixel2Mesh. GAT can assign different weights to different nodes and eliminate the noise of graph structure data. By calculating the current node and the attention coefficient of neighbors, the graph neural network can pay more attention to important nodes to reduce the impact of edge noise, which can make deformation better.

2. Related work

The traditional 3D reconstruction field generally uses multi-view geometry (MVG) [5]. The direction of MVG mainly includes SFM [6] and SLAM [7]. SFM is a passive monocular vision algorithm. SFM only uses a single camera as the acquisition device, which has the advantages of low cost and easy deployment. SLAM requires real-time and is often used for navigation and positioning. MVG cannot reconstruct the invisible part of the object, so it usually takes a long time to get enough views for a good reconstruction.

The 3D reconstruction of deep learning has made great

progress due to the release of large 3d data sets such as ShapNet. There are three methods for directly using deep learning algorithms for 3D reconstruction: point cloud, voxel, and mesh. Qi et al. [8] used point cloud as a representation for identifying deep learning tasks for the first time. Fan et al. [9] used point clouds to make a 3D reconstruction. The voxel representation is relatively simple but the accuracy is limited by memory. Due to memory limitations, there is some work to perform voxel reconstruction with multi-resolution, which is also difficult. The rich details represented by the mesh have a better effect. N. Wan and others proposed an end-to-end deep learning structure[1]. Based on the structure of Pixel2Mesh, we add an attention mechanism.

3. Method

3.1. System overview

The overview of the 3D reconstruction structure which generates a 3D mesh from a single picture is in Figure 2. Input the system single RGB picture and an initial ellipsoid represented by graph network. CNN can extract the features of pictures well. We use CNN to extract features from the picture and perceptual features to integrate two-dimensional features into three-dimensional shape features

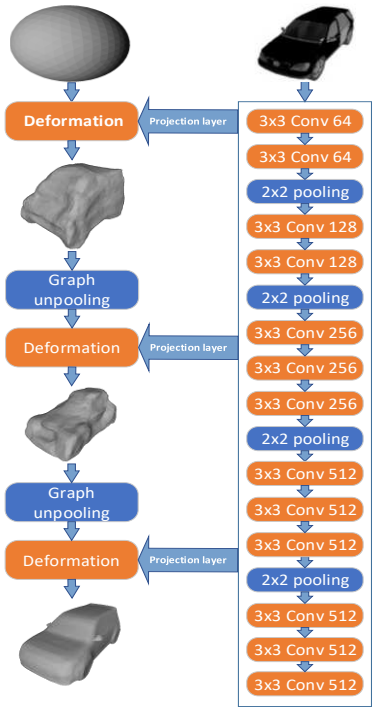


Fig.2 This is the entire 3D reconstruction process.

3.2. Graph attention network

we also introduced an attention mechanism in the graph network. Graph attention network can assign different weights to different nodes and make the characteristics of the nodes independent of the structure of the graph so that the model has better generalization. The self-attention mechanism is implemented for each node and the attention coefficient is:

$$e_{ij} = a(W\vec{h_i}, W\vec{h_j}) \tag{1}$$

e_{ij} expresses the importance of node j to node i without considering the information of the graph structure. The attention mechanism a is a single-layer feedforward neural network. W is the weight matrix obtained by training. $\vec{h} = \{h_1, h_2, \cdots, h_n\}$ is the feature vector of the node. e_{ij} only allocates attention to the neighbor node set N_i of nodes i. To make the attention coefficient easier to calculate and facilitate comparison, we introduce a softmax function to regularize all the adjacent nodes j of i.

$$softmax_i(e_{ij}) = \frac{exp(e_{ij})}{\sum_{k \in Ni} exp(e_{ik})} \tag{2}$$

In the end, we get the complete attention α_{ij} mechanism as follows:

$$\alpha_{ij} = \frac{exp(LeakeReLu(\vec{a}^T [W\vec{h_i} \| W\vec{h_j}]))}{\sum_{k \in Ni} exp(LeakeReLu(\vec{a}^T [W\vec{h_i} \| W\vec{h_k}]))} \tag{3}$$

$\vec{a}$ is the weight matrix between the connection layer and the layer in the neural network. The LeakyReLu function which assigns a no-zero 0.2 slope to all negative values is added to the output layer of the feedforward network. The attention coefficient can be used to predict the output characteristics of each node

3.3. Projection layer

The VGG16 network is used to extract the picture features. To use the feature of the picture in the 3D mesh, projection mapping is required. The projection layer projects three-dimensional coordinates onto a plane. Use bilinear interpolation to calculate new feature points for the four pixels adjacent to the projection point. The formula for bilinear interpolation is as follows:

$$\begin{aligned} \vec{R_1} &= \frac{x_2 - x}{x_2 - x_1} \vec{Q_{11}} + \frac{x - x_1}{x_2 - x_1} \vec{Q_{21}} \\ \vec{R_2} &= \frac{x_2 - x}{x_2 - x_1} \vec{Q_{12}} + \frac{x - x_1}{x_2 - x_1} \vec{Q_{22}} \\ \vec{P} &= \frac{y_2 - y}{y_2 - y_1} \vec{R_1} + \frac{y_2 - y}{y_2 - y_1} \vec{R_2} \end{aligned} \tag{4}$$

$\overrightarrow{Q_{ij}}$ is the feature vector corresponding to the four adjacent pixels q_{ij} of the projection point p. The feature $\overrightarrow{Q_{ij}}$ extracted by VGG16 from the picture has 1280 dimensions. First, interpolate the vectors R_1 and R_2 in the horizontal direction. Then interpolate in the vertical direction to calculate vector P.

3.4. Deformation block

The attention coefficient between different nodes after regularization can be used to predict the output characteristics of each node.

$$\overrightarrow{h^{l+1}}_i = \sigma(\sum_{j \in Ni} \alpha_{ij} W \overrightarrow{h_j}) \tag{5}$$

W is the weight function obtained by training. α_{ij} is the calculated correlation coefficient of attention. σ is the nonlinear activation function. The formula defines the process of updating the feature vector of the l layer to obtain the feature vector of the $l+1$ layer, which is equivalent to performing deformation.

3.5. Graph unpooling layer

The graph unpooling layer function is to gradually increase the number of vertices in the 3D mesh. Because the direct generation of high-precision mesh will take up too much memory and affect the quality of the generation. The graph unpooling layer adds endpoints at the center of the triangle sides and then connects the endpoints.

3.6. Loss

We use three loss functions: chamfer distance, Normal loss, Laplacian Regularization. x is the predicted mesh vertex, y is the corresponding vertex on the ground truth. $N(y)$ is the neighboring pixel. The three loss functions are as follows.

Chamfer distance: Chamfer distance is used to limit the position of the mesh vertices.

$$l_{CD} = \sum_x \min_y \| x - y \|_2^2 + \sum_y \min \| y - x \|_2^2 \tag{6}$$

Normal loss: the function is used to enhance the normal consistency of the mesh surface and increase the smoothness. $k \in N(y)$ is the adjacent pixel of y, $<,>$ is the inner product of two vectors, n_y is the surface normal observed from the ground truth.

$$l_n = \sum_x \sum_y = \arg\min_y (\| y - x \|_2^2) \| < y - k, n_y > \|_2^2 \tag{7}$$

Laplacian Regularization: it is used to maintain the relative position of the vertex so that the vertex position cannot be changed too freely. λ_x is a laplacian coordinates. We use the weighted sum of the three-loss functions as the final loss function: $l_{total} = l_{cd} + \lambda_1 l_n + \lambda_2 l_{lap}$. $\lambda_1 = 0.3$, $\lambda_2 = 0.3$.

$$\lambda_x = y - \sum_{k \in N(x)} \frac{1}{\| N(x) \|} k$$
$$\sum_x \| \lambda'_x - \lambda_x \|_2^2 \tag{8}$$

4. Experiment

In this part, we will compare the accuracy of the model reconstructed by the graph attention network with Pixel2Mesh and show our different kinds of reconstruction results. In addition to using the Shapenet dataset[10], we also use real pictures for reconstruction. We have some analysis and conjectures about the real reconstruction results

4.1. Experimental setup

Dataset: We use the Shapenet dataset provided by Choy et al.[2]. The dataset contains images that render 50k models belonging to 13 object categories in ShapeNet. We divide the data set into training and a validation set, on which we can track the loss of the method and all baselines to determine when to stop training.

Baseline: For the 3D reconstruction of a single image, we mainly added an attention mechanism to the Pixel2Mesh graph network. Compare on the Shapenet dataset.

Metrics: To evaluate the 3D reconstruction model, we use IoU and Chamfer-L1 distance. The volume IoU is defined as the quotient of the volume of the union of two meshs and the volume of the intersection. We randomly sample 100k points and determine whether these points are outside the ground truth. The bigger the IOU, the better, and the ideal situation is to completely overlap. Chamfer-L1 distance defines the average distance from a point on the output mesh to the nearest point on the ground truth mesh. By randomly sampling 100k points from the two meshs and using the KD tree to estimate the corresponding distance, we can effectively estimate the two distances. For chamfer-L1 smaller is better.

4.2. Results

The results of metrics are in Table 1 and the reconstruction results are shown in Figure 3. In Table 1, we use IoU and CD as evaluation indicators. Our performance level has reached the baseline level. Some categories have better results. In Figure 3, there are six reconstructions of common items. The reconstructed mesh model has good accuracy.

Table 1 Comparison to Pixel2Mesh.

	IoU↑		CD↓	
Category	P2M	Ours	P2M	Ours
car	0.521	**0.526**	**0.266**	0.262
chair	**0.362**	0.360	0.586	**0.584**
table	0.350	**0.353**	**0.470**	0.472
plane	**0.369**	0.365	0.467	**0.468**
couch	**0.571**	0.569	**0.493**	0.490
phone	0.615	**0.618**	0.433	**0.431**
mean	**0.465**	**0.465**	**0.452**	**0.451**

Fig.3 3D models of some classes generated from a single RGB picture.

4.3. Reconstruction of real-world pictures

We reconstruct the results based on the pictures on the Internet(Figure 3). Compared with the reconstruction results of the Shapenet dataset, some real pictures have good reconstruction results, and some are worse. We suspect that the neural network may learn classification rather than reconstruction. Real pictures similar in style to the training set may perform better.

Fig.4 3D reconstruction from real image.

5. Conclusions

Based on the general network architecture of Pixel2meh, we generate a 3D mesh end-to-end from a single RGB image. We use a graph neural network to represent the 3D mesh, and an attention mechanism is introduced during deformation. GAT can assign different weights to neighbor node features, which can better deform the ellipsoid. Our reconstructed mesh has good accuracy on the Shapenet dataset. Some pictures from the real world have good reconstruction results, some are not good. How to make the network learn to reason about the shape and contour of the 2D object in the picture is a question worth considering.

Acknowledgments

This work supported by National Key R&D Program of China (2019YFB1406202) and supported by Sichuan Science and Technology Program (2019ZDZX0009)

References

[1] Nanyang Wang, Yinda Zhang, Zhuwen Li, Yanwei Fu, Wei Liu, Yu-Gang Jiang, “Pixel2Mesh: Generating 3D Mesh Models from Single RGB Images”, Proceeding of ECCV, pp. 52-67, 2018.

[2] Choy, C.B., Xu, D., Gwak, J., Chen, K., Savarese, S.: 3d-r2n2, “3d-r2n2: A unified approach for single and multi-view 3d object reconstruction”, Proceeding of ECCV, pp 628-644, 2016.

[3] Haoqiang Fan, Hao Su, Leonidas J. Guibas, “A point set generation network for 3d object reconstruction from a single picture”, Proceeding of CVPR, pp. 605-613,2017

[4] Petar Veličković, Guillem Cucurull, Arantxa Casanova, Adriana Romero, Pietro Liò, Yoshua Bengio. “Graph Attention Networks”, Proceeding of ICLR(2018).

[5] Hartley, R., Zisserman, A., “Multiple View Geometry in Computer Vision”, Cambridge University Press (2004).

[6] Sch¨onberger, J.L., Frahm, J., “Structure-from-motion revisited”, Proceeding of CVPR (2016).

[7] Cadena, C., Carlone, L., Carrillo, H., Latif, Y., Scaramuzza, D., Neira, J., Reid, I., Leonard, J.:Past, present, and future of simultaneous localization and mapping: Towards the robust-perception age. IEEE Transactions on Robotics32(6), 1309–1332 (2016).

[8] C. R. Qi, H. Su, K. Mo, and L. J. Guibas, “PointNet: Deep learning on point sets for 3D classification and segmentation” In Proc. CVPR, 2017.

[9] H. Fan, H. Su, and L. J. Guibas. A point set generation network for 3D object reconstruction from a single image. In Proc. CVPR, 2017.

[10] Angel X Chang, Thomasn Funkhouser, Leonidas Guibas, et al. Shapenet: An information-rich 3d model repository. arXiv preprintarXiv:1512.03012, 2015.

ELABORATION ON OCCUPANCY NETWORKS AND RESIZING STRATEGY

SONG SHENGYU[1], GU XIAOFENG[1], KUANG PING[1], XU YUANYUAN[1],

[1] School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China

E-MAIL: 202022090502@std.uestc.edu.cn, kuangping@uestc.edu.cn, guxf@uestc.edu.cn, hyries@std.uestc.edu.cn

Abstract:

Occupancy networks introduces the decision boundary of neural network classifier to express arbitrarily complex three-dimensional topological structure, thereby solving the problem of incompatibility between the efficiency of calculation and the validity of storage in the field of 3D reconstruction. We briefly introduced the principle of occupancy network and its single-object 3D reconstruction effect. When further applying occupancy network to real online images, we propose a feasible resizing strategy to improve the versatility of occupancy network. We believe this will help occupancy network move towards a broader scene.

Keywords:

3D reconstruction; Occupancy Networks; Single object; Resizing strategy;

1. Introduction

3D reconstruction is a research hotspot of computer graphics[1-3], which aims to recover geometric models from a given image dataset. Recently, learning-based 3D reconstruction methods have attracted attention and produce many refreshing research results. Brock et al. contributed methods for training voxel-based variational autoencoders[1]. Fan et al. introduced point clouds to represent 3D output[4]. Aiming at the three-dimensional surface simulation problem, Liao et al. conducted in-depth research on the marching cube method, and finally realized the high-resolution construction of various three-dimensional structures[5].

Nevertheless, existing 3D output representations are not compatible with the efficiency of computation and the ability to express high-resolution geometric figures of arbitrary topology. Here we will introduce a 3D graphics generation technology called Occupancy Networks.

Mescheder et al. proposed Occupancy Networks creatively in last year[6]. Occupancy Networks can solve the incompatibility problem mentioned above and is applicable in scenes with point cloud, voxel, etc. as input. In this article we introduce the Occupancy Networks and our experimental results. Further, we propose a strategy that can improve the versatility of occupancy network.

2. Method

In this section, the construction method of occupancy network will be briefly described. Further, we will show how it is utilized in 3D reconstruction practice.

2.1. Occupancy Networks

For every possible point $p \in \mathbb{R}^3$ in three-dimensional space, occupancy function assigns occupancy probability between 0 and 1. The function is as follows:

$$o : \mathbb{R}^3 \to \{0,1\} \tag{1}$$

To approximate this 3D function, the key tool is the neural network. Occupancy Networks utilizes a Peer-to-peer mapping. Take estimated occupancy of three-dimensional space points $x \in \mathcal{X}$ as a part of input. And It is further spliced with selected points to form the original mapping image $(p, x) \in \mathbb{R}^3 \times \mathcal{X}$. The mapping from $p \in \mathbb{R}^3$ to $\mathbb{R}$ outputs the corresponding image which is a value between 0 and 1. This input to output mapping relationship can be parameterized by a neural network f_θ :

$$f_\theta : \mathbb{R}^3 \times \mathcal{X} \to [0,1] \tag{2}$$

2.2. Training

In order to obtain the mapping coefficients θ of the f_θ, the random sampling method is used here for the 3D body edge of observed target. More specifically, in the i-th training process trainer extracts K spots $p_{ij} \in \mathbb{R}^3, j=1,\ldots,K$. Calculate the minimum of the loss $\mathcal{L}_b$ afterwards:

$$\mathcal{L}_b(\theta) = \frac{1}{|b|}\sum_{i=1}^{|b|}\sum_{j=1}^{K}\mathcal{L}\left(f_\theta(p_{ij}, x_i), o_{ij}\right) \tag{3}$$

Here, x_i is the i'th point-group of b, o_{ij} indicates the probability of existence at spot p_{ij}. $\mathcal{L}(.,.)$ is the cross entropy loss.

2.3. Multiresolution IsoSurface Extraction

Then we introduce Multiresolution IsoSurface Extraction (MISE), an isosurface extraction algorithm with progressive accuracy. MISE can refine high-resolution grids through gradually constructing an octree[8,9]. Simultaneously, we only need to estimate the occupancy grid for part of high-dimensional points, which helps improve efficiency of computation.

We first voxelize the three-dimensional space. Next, we map the input to get the occupancy network $f_\theta(p, x)$ of all p in the voxelized three-dimensional space. All grid spots p with a greater probability than a certain threshold τ will be recorded. Next, we mark all voxels that have multiple spots with different occupied probability as active ones. If we apply the marching cube algorithm at the current resolution, these voxels will intersect the grid. Make voxels will be divided equally to gain 8 sub-voxels. Then estimate proprietorial new grid spots generated through the division step. We iteratively perform the above process until the target resolution is reached. Finally, we introduce the following mathematical form to express an isosurface.

$$\{p \in \mathbb{R}^3 \mid f_\theta(p, x) = \tau\} \tag{4}$$

In general, it takes 3s to extract a grid from the occupancy network.

3. Experiments

We will introduce the content of this section in two parts. First, we reveal evaluation results of the performance of the occupancy network and the extent to which it solves the problems we mentioned in the introduction.

3.1. Dataset

For experiments Mescheder et al.[6] used the ShapeNet [7] subset of Choy et al.[2]. ShapeNet is a large, annotated library of 3D objects[7]. ShapeNet includes 3D models that belong to multiple semantic classification. It is a collection of datasets that provide many semantic annotations for each 3D model, for instance, precise alignment of spatial features, smooth and uniform double-sided surfaces, physical dimensions, keywords, and other planned annotations.

3.2. Metrics

For evaluation, Mescheder et al.[6] selected the following three-dimensional topological indicators.

Volumetric IoU: The full name of IoU is Intersection over Union. IoU calculates the quotient of union of the "estimated bounding box" and the "true bounding box" and the overlap. Correspondingly elaboration on volumetric IoU here is the ratio of predicted and actual 3D models' intersection and their union.

Chamfer-L_1 Distance: The definition of Chamfer-L_1 distance is the average of the accuracy and incompleteness measures. The definition of the accuracy here is the average length from a point on the 3D reconstruction grid to the most adjacent point in the real model data. Chamfer-L_1 distance is mainly used for point cloud reconstruction or 3D reconstruction. It is defined as follows:

$$d_{CD}(S1, S2) = \frac{1}{S1}\sum_{x \in S1} \min_{y \in S1} \|x - y\|_2^2 + \frac{1}{S1}\sum_{x \in S1} \min_{y \in S1} \|x - y\|_2^2 \tag{5}$$

Normal Consistency: In order to measure the degree to which these algorithms extract higher order conditions, the consistency assessment is defined of normal on one grid, the product of absolute values, and the normal of the most adjacent neighbors on another grid.

In our continuation experiment, we utilized input data from network sources.

Online Products data: These data are pictures of products we randomly sampled on the Internet. In next section, we will introduce the problems that we encountered when using these data for single-object 3D reconstruction and elaborate on our strategy which makes the occupancy network work better.

3.3. Results

First, we used occupancy network to perform a single-object 3D reconstruction task. We reconstructed eight types of objects and got the results. The reconstruction results is shown in the figure below. From these results, we can see that the method of occupancy network can catch complicated shapes, generate complete grid and retain particulars to the greatest extent.

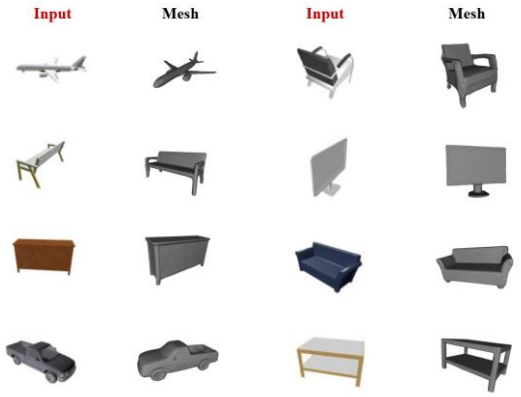


Fig.1 Single Object 3D Reconstruction.

Images of the reconstruction task is marked in red font. And the eight types all come from the ShapeNet dataset.

In table 1[6], the performance evaluation results of occupancy network have reached the most advanced standards when it was published. And for IoU, the excellent characteristics of occupancy network is also reflected in its realization of higher IoU does not depend on the number of parameters.

4. Our Problem and Strategy

When we observe the excellent performance of occupancy network, we naturally want to apply it to more 3D reconstruction practices.

Table 1 Performance Evaluation.

But when the resolution and size of the real images are far different from the images in the data set, the 3D reconstruction effect of occupancy newwork appears to be significantly reduced. The following figure can intuitively reflect the decline of its 3D reconstruction effect. Based on OpenCV, we designed a strategy to adjust the pixels of the input images to make it close to the form of the ShapeNet dataset.

category	IoU	Champer-*L*	Normal Consistency
airplane	0.571	0.147	0.840
bench	0.485	0.155	0.813
cabinet	0.733	0.167	0.879
car	0.737	0.159	0.852
chair	0.501	0.228	0.823
display	0.471	0.278	0.854
lamp	0.371	0.479	0.731
loudspeaker	0.647	0.300	0.832
rifle	0.474	0.141	0.766
sofa	0.680	0.194	0.863
table	0.506	0.189	0.858
telephone	0.720	0.140	0.935
vessel	0.530	0.218	0.794
mean	0.571	0.215	0.834

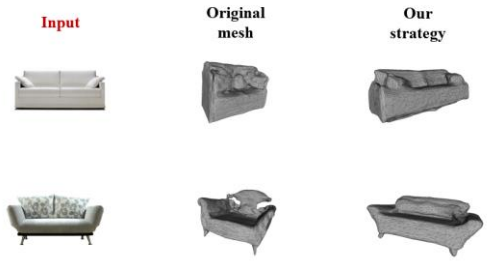


Fig.2 Sofa Resizing.

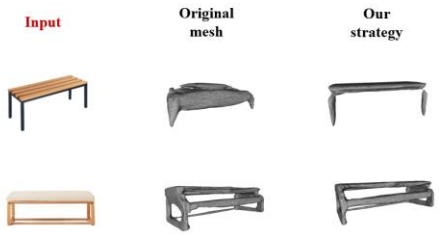


Fig.3 Bench Resizing.

As shown in Fig.2 and Fig.3, we have verified our strategy through the practice of 3D reconstruction of sofas and benches. For product images from the Internet, the performance of occupancy network is not as usual, but there is a significant decline and distortion. The redundant information of the mesh is well cleaned up. By resizing the input images, we get better 3D reconstruction results. Our strategy allows occupancy network to be more effectively applied to a wider range of scenarios.

5. Conclusions

Mescheder et al. proposed Occupancy Networks creatively that can capture complex topologies, generate closed meshes and retain most details. We introduced the actual principle of occupancy network and its experimental results on the dataset. According to the mentioned metrics and the actual generated meshes, occupancy network undoubtedly performs well on datasets such as ShapeNet.

When we tried to apply occupancy network to a wider range of online product images, its performance dropped significantly. Then we introduced our response strategy and verification results. We believe that this will enhance the versa-

tility of occupancy network and adapt it to more 3D reconstruction tasks.

Acknowledgements

This work supported by Sichuan Science and Technology Program (2019ZDZX0009 、 2019YFG0492 、 2019ZDZX0005)

References

[1] A. Brock, T. Lim, J. M. Ritchie, and N. Weston, “Generative and discriminative voxel modeling with convolutional neural networks”,arXiv.org, 1608.04236, 2016.

[2] C. B. Choy, D. Xu, J. Gwak, K. Chen, and S. Savarese, “3D-R2N2: A unified approach for single and multi-view 3D object reconstruction”, Proceeding of the European Conference on Computer Vision (ECCV), 2016.

[3] R. Girdhar, D. F. Fouhey, M. Rodriguez, and A. Gupta, “Learning a predictable and generative vector representation for objects”, Proceeding of the European Conference on Computer Vision (ECCV), 2016.

[4] H. Fan, H. Su, and L. J. Guibas, “A point set generation network for 3D object reconstruction from a single image”, Proceeding of IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2017.

[5] Y. Liao, S. Donne, and A. Geiger, “Deep marching cubes: Learning explicit surface representations. In Proc”, Proceeding of IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018.

[6] L. Mescheder, M. Oechsle, M. Niemeyer, S. Nowozin, A. Geiger, “Occupancy Networks: Learning 3D Reconstruction in Function Space”, arXiv.org, 1812.03828v2, 2019.

[7] A. X. Chang, T. A. Funkhouser, L. J. Guibas, P. Hanrahan, Q. Huang, Z. Li, S. Savarese, M. Savva, S. Song, H. Su, J.Xiao, L.Yi, F.Yu, “ShapeNet: Aninformation-rich 3D model repository”, arXiv.org, 1512.03012, 2015.

[8] C. L. Jackins and S. L. Tanimoto, “Oct-trees and their use in representing three-dimensional objects”, Computer Graphics and Image Processing, 14(3):249–270, 1980.

[9] D. Meagher, “Geometric modeling using octree encoding”, Computer graphics and image processing, 19(2):129–147, 1982.

A CASCADING INCREMENTAL TRAINING APPROACH FOR LARGE-SCALE DISTRIBUTED DATA BASED ON SUPPORT VECTOR MACHINE

XU YUANYUAN[1], LI SHUCHENG[2], LI FAN[1], GU XIAOFENG[1], SUN RUI[3]

[1]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China
[2]Sichuan shengtian new energy development co., ltd. No.333, East Section of HuPan Road, Tianfu New Area, Chengdu 610213, China
[3]School of Mechanical and Electrical Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
E-MAIL: hyries@std.uestc.edu.cn, lishucheng@scshengtian.com, lifan@uestc.edu.cn, guxf@uestc.edu.cn, rispper@uestc.edu.cn

Abstract:

In this paper, we present a cascading incremental training approach for large-scale and unevenly distributed data based on Support Vector Machine. Instead of using training data directly, data's distribution and scale are concerned， so Synthetic Minority Oversampling Technique and Generative Adversarial Networks are both used to synthesize new samples and add them to the data set to achieve a balanced sample number. Then, we propose a cascading model and divide samples into groups and apply the multi-layer convolutional neural network for pre-training to collect the embedding vectors of training samples. Finally, features extracted from the pre-training will be used for incremental training on Support Vector Machine. A multi-layer convolutional network and cluster are applied to maintain some key information and train features for classification. Additionally, uncertainty strategy is used to obtain potential features. In the comparative experiments with the above dataset, our proposed method performs the state-of-the-art competitors.

Keywords:

Incremental learning; Classification; Cascade model; Convolutional network; Clustering; Support Vector Machine

1. Introduction

Support vector machines (SVMs)is a classic and popular technique for its high performance in many fields of machine learning and artificial intelligence, which is proposed by Dr. Vapnik[1]and his research team. SVMs classifies through mapping the training samples to high-dimensional space. Then a hyperplane is constructed in this feature space, which divides the different categories into two and maximizes the distance between itself and the point closest to it. This decision surface can be used as the basis of unknown classification vector classification. The advantage of support vector machine is that it can prevent overfitting. SVM is a convex optimization problem, so the local optimal solution must be the advantage of the global optimal solution. The training SVM requires a coefficient equal to the number of training examples to solve the quadratic programming (QP) problem. For large scale datasets, QP's standard numerical techniques become infeasible[2][3].Therefore we can take advantage of the incremental training approach for the natural properties of SVM. The incremental training has two merits:1) Discarding some old data to reduce the storage cost;2) Past training results help speed up the next training[4]. In the past, many people combined incremental training with support vector machines, applied them to many scenarios, and achieved good results. In this paper, we mainly focus on large scaled and unevenly distribution dataset with a cascading incremental training approach on SVM. Our proposed method can effectively overcome some shortcomings of existing methods and improve accuracy. The structure of this paper as follows: Chapter2 our proposed approach will be introduced. Then Chapter3 is experiments results and analysis. Finally, Chapter4 is the conclusion.

2. The Proposed Cascading Incremental Training Approach

The proposed approach is a cascading model，before dividing the dataset into several sub-data and doing classification task for samples，it uses the SMOTE algorithm to analyze the minority samples to get k neighboring samples, and use GANs to build new samples to achieve positive and negative samples balance. Then, a multi-layer convolutional network is applied for embedding x_i into a

feature space, obtaining effectively information than using the samples directly. During the incremental training, we should concern four kinds information, they are support vectors (SVs), Non- support vectors (Non-SVs) of the previous training vectors and wrong classified and correctly classified vectors of the next data set. SVs of the previous training data set act as the basis for the current solution; Non-SVs of the previous training data set hardly works in this training, However, when new information is added, a few portion of them has a probability of turning into SVs; the wrong classified samples of the next data set describes the next data changes emphatically, providing new information for the next SVM solution; the correctly classified samples of the next data is unable to provide valid information to the new classifier, while a small percentage of them may become SVs in incremental training too.

In summary, the importance of the above four different information is as follows$\{SVs\} \geq \{Wrongclassified\} > \{Non-SVs\} \geq \{Correctlyclassified\}$

First of all, to the data set may be large and unevenly distributed, we mainly consider the unevenly distribution of samples. We use the SMOTE algorithm to analyze the minority samples and GANs synthesize new samples based on the minority samples and add them to the data set. Then we use a multi-layer convolutional network embedding the samples of sub-set into a feature space to extract the effectively information and a clustering to extract and get the distribution information. At the same time, with the uncertainty strategy, some further useful or potential samples can be extracted. Through the above methods, we can get distribution information in the data. With the experiments, our proposed the cascading incremental training approach can be proved have a better performance.

2.1. Synthesizer

In large-scale datasets with uneven distribution, there is usually a large difference in the number of positive and negative samples. We use SMOTE and GANs to analyze a small number of samples and synthesize new samples to achieve sample homogeneity. For example, if the ratio of positive samples to negative samples is 20:1, then we can generate 19 negative samples to reach the ratio of positive samples to negative samples at 1:1, and then carry out the following training task.

First, for each sample in the minority class, we use the Euclidean distance as the standard to calculate the distance from all samples in the minority class sample set to get its k proximity; then, set a sampling ratio according to the sample imbalance ratio to determine the sampling ratio N, for each minority x,randomly select several samples from the vicinity of k to form a new training set K, and then use a GAN-based synthesizer to synthesize the examples and add them to the original data set, which can be constructed as

$$\min_G \max_D E_{x\in K}[\log D(x)] + E_{x\in G(z)}\left[\log\left(1 - D(x')\right)\right] + \mu E_{x'\epsilon G(z)}\left[D_{KL}\left(\upsilon(y')||P_\theta(\hat{y}|x')\right)\right] \quad (1)$$

Where$D(x), G(x)$are discriminator and generator; are samples from a new training set k and synthesized set ;z is gaussian distribution;$E_{x\in k}\left[log\left(D(x)\right)\right] + E_{x\epsilon G(z)}\left[log\left(1 - D\left(x\right)\right)\right]$ make the synthesized instances has the same distribution as the original samples; D_{KL} attempts to make synthetic instances classified by P_θ have less confidence.

2.2. Pretraining of multilayer convolutional network

Our proposed method uses two kinds of technologies to obtain the data's distribution information, A multi-layer convolutional network and a clustering.

We suppose that the samples in our data set are in vector form, we can change the shape of all samples into an $M \times M$ matrix and fill in the missing values. Suppose the given dataset is $\{(x_i, y_i), \dots, (x_n, y_n)\}, i = 1,2, \dots, n, x_i \in R^{M\times M}, l_i \in \{1, \dots, K\}$,where x_i is a sample from sub-data set and l_i is its label, K is the number of the sub-data set. x_i is mapped to a feature space through a multi-layer convolutional network H and the extracted features are then classified through multiple full connection layers C. The well-known cross entropy will be used as the loss function

$$loss_{classify}(\theta_H, \theta_C) = -\sum_{i=1}^{N}\sum_{k=1}^{K} P_k(l_i)\log q_k(x_i) \quad (2)$$

Where θ_H, θ_C are the parameter set of convolutional networks H and classifier C. When label k is l_i, $p_k(l_i)$ represents 1, and when label k is not l_i, $p_k(l_i)$ represents 0. $q_k(l_i)$ is the probability of being divided into k by the classifier C.

2.3. Clustering

Clustering is a technique that divides a group of sample data into several different categories, among which the samples of the same category have high similarity and the samples of different categories have great differences. According to different data types and clustering purposes, the clustering algorithms selected are quite different. The well-known clustering algorithms include K-means, hierarchical clustering, SOM clustering, FCM clustering, etc.

To improve the effect of the classifier, we take two samples $(x_i^+, l_i^-), (x_i^-, l_i^-)$ for each x_i at random, where $l_i^+ = l_i, l_i^- \neq l_i$. First of all, the features of x_i, x_i^+, x_i^- are

extracted by multi-layer convolutional network H as follows

$$f_i = H(x_i), f_i^+ = H(x_i^+), f_i^- = H(x_i^-) \quad (3)$$

We assume that samples with same characteristics should be closer , while samples with different characteristics should be separate. Based on this assumption, we can train the samples with the same characteristics closer and the samples with different characteristics farther as follows

$$\min_{\theta_H} ||f_i - f_i^+||_2, \max_{\theta_H} ||f_i - f_i^-||_2 \quad (4)$$

So, the loss function on clustering can be expressed as

$$loss_{cluster}(\theta_H) = \sum_{i=1}^{N} (||f_i - f_i^+||_2 - ||f_i - f_i^-||_2) \quad (5)$$

Where$||\cdot||$is Euclidean distance,$||f_i - f_i^+||_2$and$||f_i - f_i^-||_2$are both trained to decrease with the gradient descend of the loss function, so the classes of the same label will close to each other more and more and classes of the different label will keep away from each other.

2.4. Uncertainty Strategy

In order to select the samples from the correctly classified data in the new subset that are most likely to be converted into SVs in the next training, we propose to rank the samples based on an uncertainty strategy. Entropy is the expected value(average) of the information contained in each message received. It is conceivable that the greater the entropy value, the greater the degree of information change.

Assuming that the dataset consists of n samples, each sample contains m-dimensional information, and x_{ij} represents the $i-th$ sample of the $j-th$ dimension, as shown below, each sample is processed by non-negative and translational processing

$$x_{ij} = \frac{x_{ij} - min(x_{1j}, \dots, x_{nj},)}{max(x_{1j}, \dots, x_{nj},) - min(x_{1j}, \dots, x_{nj},)} + 1 \quad (6)$$

$$p_{ij} = \frac{x_{ij}}{\sum_{i=1}^{n} x_{ij}} \quad (7)$$

Where p_{ij} represents the weight of $i-th$ sample in $j-th$ dimension. The entropy of $j-th$ can be expressed as

$$e_j = -\frac{\sum_{i=1}^{n} p_{ij} \ln(p_{ij})}{\ln(n)}, (0 \le e_j \le 1) \quad (8)$$

Then we can obtain the diversity factor and the weight of $i-th$ dimension as follow

$$g_i = \frac{1-e_j}{m-\sum_{j=1}^{m} e_j}, (0 \le g_j \le 1, \sum_{j=1}^{m} g_j = 1) \quad (9)$$

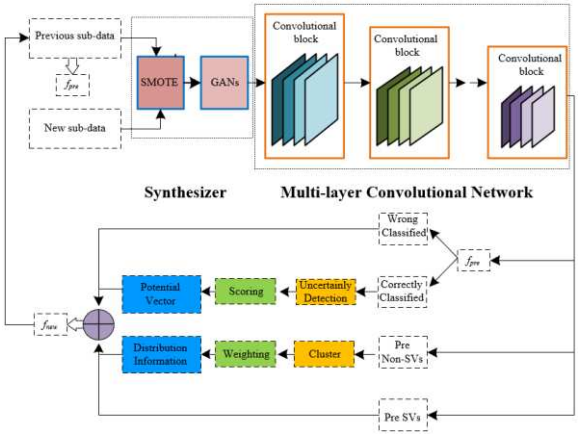
$$w_j = \frac{g_j}{\sum_{j=1}^{m} g_j}, (1 \le j \le m) \quad (10)$$

Finally, the samples' scores can be expressed as

$$s_i = \sum_{j=1}^{m} w_j p_{ij}, (i = 1, \dots, n, j = 1, \dots, m) \quad (11)$$

We can sort these samples by a ranking of samples, and the samples with higher score can be separated and added to the new training set.

2.5. Framework and Model Structure of Proposed Method



3. Experiments

In this experiment, two datasets with different scales and uneven distribution that are widely used in the field of SVM-based incremental learning are ready to be used[5][5]. They are Banana dataset from IDA benchmark repository and Skin Segmentation dataset from UCI machine learning. Among them, the Banana dataset is small, with 8800 training samples and 1000 test samples; the Skin dataset is larger, with a total of 245057 samples, of which 50859 samples are skin samples and 194198 samples are non-skin samples. In this experiment, 4 evaluation criteria are included: Accuracy (ACC), Precision(PRE), Specificity(SPE) and False Positive Rate(FPR).

Firstly, compare our proposed method with Redundant-ISVM[6]and the KKT-ISVM[7]commonly used in the Banana dataset.

Table 1 Comparison with current ISVM in Banana

Banana	Proposed	Redundant	KKT
ACC	0.9060	0.8600	0.8200
PRE	0.9087	0.7946	0.7409
SPE	0.9208	0.7830	0.7038
FPR	0.0792	0.2170	0.2962

Obviously, the cascading incremental training method we proposed has better performance on the Banana dataset.

Table 2 Comparison with current ISVM in Skin Segmentation

Skin Segmentation	Proposed	Redundant	KKT
ACC	0.9986	0.9970	0.9970
PRE	0.9998	0.9995	0.9995
SPE	0.9999	0.9998	0.9998
FPR	4.6430e-5	1.7873e-4	1.7873e-4

Then we compare these algorithms on the large data set Skin Segmentation. From the four evaluation criteria, we can see that our proposed model, a cascading incremental approach, performs better on the large data set.

Table 3 Comparison with current ISVM in Banana

Banana	Batch Training	Proposed ISVM
ACC	0.9070	0.9060
PRE	0.9255	0.9087
SPE	0.8893	0.9208
FPR	0.0623	0.0792
TIME	1	1.1420

Next, we compare the performance of incremental training and batch training on the banana dataset. From Table 3, we can see that there is almost no difference in accuracy between the two performances, and other evaluation criteria are also relatively similar.

Table 4 Comparison with Batch training in Skin Segmentation

Skin Segmentation	Batch Training	Proposed ISVM
ACC	0.9991	0.9986
PRE	0.9995	0.9998
SPE	0.9999	0.9999
FPR	1.3976e-5	4.6430e-5
TIME	1	0.0098

Finally, we compare incremental training and batch training on a large data set Skin Segmentation. It is obvious that the two methods are similar in performance of each parameter, but the incremental training method is more than 100 times faster than batch processing in training time. It can be seen that the computational performance of incremental training is much higher than batch processing on large and unevenly distributed data sets.

4. Conclusions

In this paper, we constructed a cascading incremental training model, while large-scale unevenly distributed datasets under analyzed. With SMOTE and GANs algorithms to balance the unevenness of the dataset samples, while a multi-layer convolutional network and likewise a clustering are used to extract the key information, and the next uncertain strategy is applied to obtain potential samples, performance on the large-scale unevenly distributed datasets will be improved on condition that the execution of incremental training. In future research work, we will further study the incremental training based on an open-set scenario which might be more common in the real world.

Acknowledgements

This work supported by Sichuan Science and Technology Program (2019GFW003、2020GFW001、2020YFG0238、2020YFG0234、2018CC0124)

References

[1] Vapnik V.N., “The Nature of Statistical Learning Theory”, Journal of Computer and Communications, Vol.4 No.10, August 10, 2016.

[2] Cauwenberghs G, Poggio T, “ Incremental and decremental support vector machine learning”, Advances in neural information processing systems, 2000, 13: 409-415.

[3] Fletcher R, Practical methods of optimization, John Wiley & Sons, 2013.

[4] Yamauchi K, Yamaguchi N, Ishii N, “Incremental learning methods with retrieving of interfered patterns”, IEEE Transactions on Neural Networks, 1999, 10(6): 1351-1365.

[5] Narendran B, Rangarajan S, Yajnik S, “Data distribution techniques for load-balanced fault-tolerant web access” ,U.S. Patent 6,070,191[P]. 2000-5-30.

[6] Wang W, “A redundant incremental learning algorithm for svm”, Proceeding of 2008 International Conference on Machine Learning and Cybernetics. IEEE, 2008, 2: 734-738.

[7] Wenhua Z, Jian M, “A novel incremental svm learning algorithm”, Proceeding of 8th International Conference on Computer Supported Cooperative Work in Design. IEEE, 2004, 1: 658-662.

CONTRASTIVE REPRESENTATION FOR DERMOSCOPY IMAGE FEW-SHOT CLASSIFICATION

MO XUAN, YANG QIANG, ZHANG XIYI, CHEN JUAN, WEN QUAN

School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
E-MAIL: chenjuan@uestc.edu.cn

Abstract:

In the field of few-shot learning, different methods are proposed to optimize the model by changing the network structure or optimizing the algorithm. Although, by designing the end-to-end algorithms, the classification performance on a specific task can be improved. But when the amount of data is limited, it is still difficult to obtain generalization ability for different tasks. At the same time，a single loss function in the end-to-end training is always ineffective，because it is difficult for a shallow network to learn an effective image feature representation from complex natural images. In this paper, a constructive representation algorithm for few-shot learning without end-to-end training is proposed, which is suitable for few-shot learning in the natural images classification task. Through self-supervised representation learning, the proposed encoding model generates an effective feature representation. Then, a few-shot learning model is further constructed and trained for supervised classification tasks. Without the end-to-end training, the proposed learning method at different training stages use different loss functions. In the experiments, on the classification task of the public competition data set ISIC2018[11], our method has a 30% performance improvement over the state-of-the-art methods.

Keywords:

Few-shot learning; Self-supervised learning; Dermoscopy image classification; Skin lesion analysis

1. Introduction

In the task of classification for dermoscopy images, we have two main difficulties. First, for some rare skin lesions, it is difficult to find a large number of image samples to make a data set. Second, it is not easy for non-professionals to distinguish different melanomas, same type of targets may have very different appearances. In order to solve these problems, we decided to use a few-shot learning method for classification and use self-supervised representation to help the model train in the case of insufficient data labels.

The most commonly used network for few-shot classification are matching networks [1] and Prototypical networks[2] .They constructed a convolution-based Siamese network structure for calculating image feature embedding. The similarity is calculated between the embedding of the positive and negative examples, then compared with the real label to obtain a contrast loss. In the aspect of feature embedding similarity evaluation, the matching network uses cosine similarity as the similarity evaluation, while the prototype network uses Euclidean distance to calculate the similarity of feature embedding.

In common few-shot learning methods [1-4], simpler network structures are usually used. It's hard for shallow networks to learn complex image semantics. This makes the usual few-shot learning methods perform well in simple target classification tasks which have similar characteristics (like handwritten characters in Ominiglot dataset); but they perform poorly on complex classification tasks (like natural image in Mini-Imagenet dataset). In the proposed methods [5-6], the representation model is trained through self-supervised methods to make the image features accepted by the downstream model easier to learn. In our method without the end-to-end training mode, few-shot classification model is performed based on the use of self-supervised image feature encoder.

2. Method

2.1. Self-supervised model construction

The CPC model mainly consists of two parts: the encoder and the autoregressive model. The training model predicts future observations from historical observations. For all images in the data set D, the feature encoder extracts the current $I_t = F_{enc}(x_t)$, at this time we have got the current observation value I_t. Then we use the autoregressor to

Corresponding Author: Chen Juan (chenjuan@uestc.edu.cn)

summarize all the observations in the historical record and generate the latent state $C_t = F_{ar}(I_{i<t})$ of the current context. After obtaining the current observation result I_t and the latent state C_t, a simple transition prediction can be constructed to predict the observation result after k steps using C_t. From this, the information relevance between the latent state C_t and the future input I_{t+k} can be quantified, which we call mutual information. The mutual information is described as a form of probability density function as follows:

$$f_k(I_{t+k}, C_t) \propto \frac{p(I_{t+k} \mid C_t)}{p(I_{t+k})} \tag{1}$$

For the description of mutual information in Eq.1, we use a logarithmic bilinear model to quantify as follows:

$$f_k(I_{t+k}, C_t) = \exp(I_{t+k}^T W_k C_t) \tag{2}$$

It can be seen that we use the linear transition matrix W_k to predict the model observations after k steps. We maximize the probability density in Eq.2 to achieve the model training goal of maximizing mutual information. We perform feature encoding and autoregression for each region blocks and select C_t as the only positive example. At the same time, we randomly extract N-1 grid feature codes $X = \{I_1, I_2, \ldots, I_{N-1}\}$ as negative examples, and perform the above encoding and autoregression operations by optimizing the following loss shown in Eq.3.

$$L_{NCE} = -\mathop{E}_{X}\left[\log \frac{f_k(I_{t+k}, C_t)}{\sum_{x_j \in X} f_k(x_j, C_t)}\right] \tag{3}$$

We define this loss function as infoNCE. From Eq.3, we can see that the loss function can be reasonably applied to the autoregressive binary classification task by randomly selecting negative examples. We process some data augmentation on the original data set, which including random clipping, color jitter, random rotation and affine transformation. For the problem of imbalance between classes, this work simply uses random rotation to expand weak classes.

After getting the trained self-supervised representation model, we use the feature encoder F_{enc} obtained by self-supervised learning to help the downstream supervised few-shot learning task to train, that is to say, we directly discard the autoregressive model F_{ar}, and only use the feature encoder to provide the feature embedding for downstream tasks.

2.2. CPC-ProtoNetwork model construction

We organize the data set substructure as follows. For the data set $D = \{D_{train}, D_{test}\}$, D_{train} is used for model training, and D_{test} is used for testing. For all data in the data set $D = \{X_i, Y_i\}_{i=1}^{N}$, Few-shot classification is performed on the isic2018 data set with support set $S_{support}$ and the query set S_{query} constructed using the M Way − N Shot method. That is, M categories are randomly sampled in the whole data set, and N samples of each category form the support set $S_{support}$; then K_{query} samples from the same M category are randomly sampled to form the support set S_{query}.

The traditional few-shot learning method (like Match Network) maps all samples to a low-dimensional feature space $\mathcal{Z}$. Then, a similarity measure $S(\cdot,\cdot)$ is used to evaluate the similarity between $f(x_{test})$ and $g(x_i)$ one by one, and the support set sample x_i label y_i with the highest similarity is assigned as the model prediction label for the query set sample x_{test}. However, in end-to-end training network uses single loss function, it is difficult to achieve the purpose of extracting features and feature space mapping at the same time, which results that the actual few-shot learning method generally performs a low classification accuracy for complex natural image.

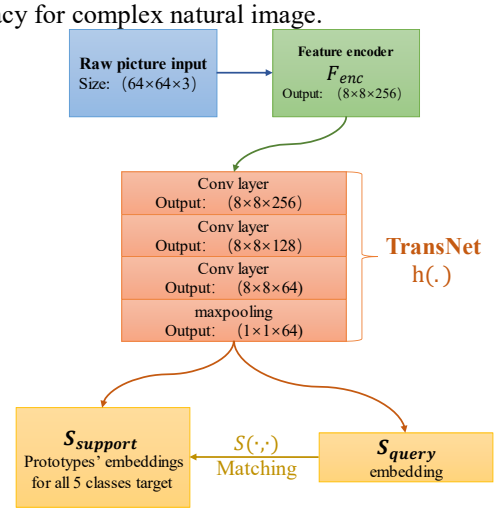


Fig.1 Proposed framework for few-shot learning

In Fig.1, we replace four-layer feature extracting network (which used in MatchNet) with the self-supervised feature encoderF_{enc}, that has been trained to map the input to the easier-to-learn semantic representation space C (Represented by green square). For generalizing the features to the embedded matching feature space $\mathcal{Z}$ (Represented by yellow square), We constructed translation network (TransNet, hereafter referred to as h(.)) for processing translation from feature space C to $\mathcal{Z}$. The structure of the TransNet is similar to the original four-layer convolutional neural network which used in MatchNet.

At the same time, in order to enhance the robustness of feature space conversion and speed up network training, we decided to use the prototype proposed by ProtoNetwork for

calculation. Which means, we pick up all samples of one class from $S_{support}$ in the feature space $\mathcal{Z}$, as the Representative, the prototype of the k-th category can be calculate as Eq.5.

$$\chi_{\mathrm{k}} = \frac{1}{|S_k|} \sum_{(x_i, y_i) \in S_k} h(F_{enc}(x_i)) \tag{4}$$

After calculating the prototype $\chi = (\chi_1, \chi_2, \cdots, \chi_M)$ for all M category, the model evaluates the similarity between every x_{test} and prototypes, then classifying them with probability in Eq.6.

$$\begin{aligned} & \mathrm{p}_\theta(y = k \mid x_{\mathrm{test}}) \\ & = \frac{\exp(S(h(F_{enc}(x_{\mathrm{test}}), \chi_{\mathrm{k}}))}{\sum_{\chi_j \in \chi} \exp(S(h(F_{enc}(x_{\mathrm{test}}), \chi_j))} \end{aligned} \tag{5}$$

Finally, we train the network by minimizing the negative log-likehood [7]. So the loss function used for stochastic gradient descent is expressed as Eq.7.

$$L_{triple} = -\log(p_\theta(y = k \mid x_{test})) \tag{6}$$

We summarize the training algorithm of the proposed model in Table 1.

Table 1 Training Algorithm for CPC-ProtoNetwork

Input : The support image set $S_{support}$ and the query image set S_{query}, given K_{query} sample images in S_{query}.
Output : The trainning loss L_{step}.

Initialize $L_{step} \leftarrow 0$
for k in {1,...,M} **do**

$$Proto_k \leftarrow \frac{1}{N} \sum_{\substack{(x_i, y_i) \in S_{support} \\ y_i = k}} h(F_{enc}(x_i))$$

end for
for k in {1,...,M} **do**
  for (x, y) in S_{query} **do**
    $innerloss \leftarrow S(h(F_{enc}(x)), Proto_k)$
    $outerloss \leftarrow log \sum_{j \neq k} \exp\left(-S(h(F_{enc}(x)), Proto_j)\right)$
    $L_{step} \leftarrow L_{step} + \frac{innerloss + outerloss}{\mathrm{M} \times K_{query}}$
  end for
end for

3. Experiments

For the experiments in this paper, the data comes from the third task of the open competition ISIC2018[11], i.e., Skin Lesion Analysis Towards Melanoma Detection (disease classification for seven categories of dermoscopy images). The public data set contains 10015 RGB images. At the same time, we compress the image to a uniform size of $64\text{pixs} \times 64\text{pixs}$ to facilitate input from different networks. For the experiment in this paper, the training set D_{train} is obtained by randomly extracting 80% of the data from each type of disease; D_{test} is obtained by extracting 10% of each type of disease; We use the remaining 10% of data to build the validation set.

3.1. Self-supervised experiment of CPC model

With reference to the original setting[4], we scale the input image to $72\text{pixs} \times 72\text{pixs}$ by linear interpolation. The model is trained by CPC, which is to divide the grid on the output feature map of the encoder F_{enc}, and perform autoregressive prediction between grid embedding. In the actual training environment, we randomly sampled 16 negative examples from 64 grids of a picture.

This experiment follows the enviroment settings of the proposed method[10], using the first three convblocks of resNet-34 to build the feature encoder F_{enc}, and constructing an autoregressive model F_{ar} with the structure of pixelCNN, just the same as CPC-V2 [5]. The autoregressive model takes the output of feature encoder (a 256-dimensional current state observation I_t) and the previous state C_{t-1} as model input. After the same 256-dimensional latent state representation C_t was calculated by autoregressive, we use the k-step transition matrix W_k multiplied C_t to predict I_{t+k}. In the actual algorithm, we set k=5, which means that our model makes predictions on the fifth grid below.

Further, we trained a convolutional network (CPC_Res101) using the feature embedding infer from F_{enc} and true label corresponding to the feature, while the comparison experiment (Res101) used the same convolutional network and loss function, but train on the raw data and label. We used the medical image classification evaluation index recommended in the isic competition to evaluate the two models. The experimental results are shown in Table 3. It can be seen that the our method(CPC_Res101) got a classification accuracy much higher than the comparison group. Our method has higher true positive rate (TPR) and true negative rate (TNR), which means The model has a low probability of mistake or omission diagnostic in the classification of skin lesions.

Table 2 Comparison result with supervised classification Methods on ISIC2018 task3 (Our method: ***CPC_Res101***)

Group name	Precision (PPV)	Recall (TPR)	TNR	FPR	F1	NPV	AUC
Res101[9]	0.6686	0.6743	0.9471	0.0529	0.6686	0.9486	0.8075
CPC_Res101	**0.8457**	**0.8486**	**0.9757**	**0.0243**	**0.8443**	**0.9771**	**0.9100**

Table 3 Comparison results for few-shot learning (Our method: ***CPC_ProtoNet***)

Group name	Precision (PPV)	Recall (TPR)	TNR	FPR	F1	NPV	AUC
MatchNet[1]	0.4920	0.4940	0.8720	0.1280	0.4900	0.8740	0.6830
ProtoNet[2]	0.6860	0.6820	0.9220	0.0780	0.6800	0.9220	0.8032
MAML[8]	0.5080	0.5100	0.8760	0.1240	0.5060	0.8780	0.6933
Reptile[3]	0.5060	0.5060	0.8740	0.1260	0.5020	0.8800	0.6921
CPC_ProtoNet	**0.9120**	**0.9120**	**0.9800**	**0.0200**	**0.9080**	**0.9820**	**0.9449**

3.2. CPC_ProtoNet model experiment

We constructed five experiments, the few-shot learning method CPC_ProtoNet,which we proposed to build 5 Way $-$ 5 Shot's support set $S_{support}$ and query set S_{query} from the data set D_{cpc}; and as comparative experimental group, MatchNet, ProtoNet, MAML [8], Reptile [3] model, built their 5 Way -5 Shot's support set and query set from D_{org}.

The network model used to extract features in other groups is completely consistent with the ProtoNet group. There are no advantages in network structure between models. After also using adam as the optimizer, setting a learning rate of 1e-3, and using 100 $S_{support}$ and S_{query} to train for 100 epochs per epoch, we get the result which is shown in Table 4. Table 4 can prove that our method (CPC_ProtoNet) uses a encoder to pre-coding the model input into a feature space that is easier to divide, so that the downstream few-shot learning model has a greatly improved classification accuracy compared to the original model.

4. Conclusions

In the algorithm we proposed, the shallow network can learn from a more effective feature space C, then getting better classification accuracy. Obviously, this training mode can be extended to other algorithms, and we will continue our research in this direction.

References

[1] Vinyals, Oriol, et al. “Matching networks for one shot learning.” Advances in Neural Information Processing Systems. 2016.

[2] Snell, Jake, Kevin Swersky, and Richard Zemel. “Prototypical networks for few-shot learning.” Advances in Neural Information Processing Systems. 2017.

[3] Nichol A, Achiam J, Schulman J. “On first-order meta-learning algorithms”. ArXiv preprint arXiv:1803.029 99.2018.

[4] Oord A, Li Y, Vinyals O. “Representation learning with contrastive predictive coding”. ArXiv preprint arXiv:1807.03748. 2018.

[5] Hénaff O J, Srinivas A, De Fauw J, et al. “Data-efficient image recognition with contrastive predictive coding.” ArXiv preprint arXiv:1905.09272. 2019.

[6] Hjelm R D, Fedorov A, Lavoie-Marchildon S, et al. “Learning deep representations by mutual information estimation and maximization”. ArXiv preprint arXiv:1808.06670. 2018.

[7] Goldberger J, Hinton G E, Roweis S, et al. “Neighbourhood components analysis”. Advances in Neural Information Processing Systems, 17: 513-520. 2004.

[8] Finn C, Abbeel P, Levine S. “Model-agnostic meta-learning for fast adaptation of deep networks”. ArXiv preprint arXiv:1703.03400. 2017.

[9] He, Kaiming, et al. "Deep residual learning for image recognition." Proceedings of the IEEE conference on computer vision and pattern recognition. 2016.

[10] Löwe, Sindy, Peter O'Connor, and Bastiaan Veeling. “Putting an end to end-to-end: Gradient-isolated learning of representations.” Advances in Neural Information Processing Systems. 2019.

[11] Noel Codella, et al. “Skin lesion analysis toward melanoma detection 2018: A Challenge Hosted by the International Skin Imaging Collaboration (ISIC).” https://arxiv.org/abs/1902.03368. 2018.

A DOMAIN ADAPTATION METHOD FOR OBJECT DETECTION IN UAV BASED ON SEMI-SUPERVISED LEARNING

SIQI LI[1], BIYUAN LIU[2*], HUAIXIN CHEN[2], ZHOU HUANG[2]

[1]Southwest China Institute of Electronic Technology, Chengdu610036, China
[2]School of Resources and Environment, University of Electronic Science and Technology of China, Chengdu611730, China
E-MAIL: *huaixinchen@uestc.edu.cn, lby9469@163.com

Abstract:

In recent years, the objects detection algorithm of deep learning neural network has been widely used in scene monitoring fields such as intelligent transportation and ground observation. But scene changes always happen caused by the seasons and the ground feature cover change, which makes the training sample (source domain) different from the application scene (target domain), and causes the original effective model to generate a lot of false alarms. This paper proposes a domain adaptation algorithm for Unmanned Aerial Vehicle (UAV) objects detection based on semi-supervised learning. Firstly applying the source domain model on target domain to generate pseudo-labels for semi-supervised learning，during fine-tuning the model with Pseudo-Label，the scale-aware loss is introduced to suppress false alarms in abnormal scale, which realize the domain adaptability of network model migration from source domain to target domain. Experiments on our dataset for monitoring ground objects show that：the proposed method avoids the catastrophic forgetting caused by the direct domain adaptation method without denoising, and maintains the target detection rate of the network model in different scenarios.

Keywords:

Objects detection in UAV; Scene change; Semi-supervised learning; Scale-aware loss; Domain adaptation;

1. Introduction

In recent years, objects detection algorithms based on deep convolutional networks [1-2] have made great progress both in speed and accuracy, such as YOLOv4[3], EfficientDet [4], etc.，and they have been widely used in scene monitoring fields such as intelligent transportation and earth observation**.**

However, this type of objects detection algorithm relies on a large amount of data for supervised training, but in some application scenarios, such as battlefield objects detection, ground target monitoring target detection, etc., it is very difficult to obtain a large amount of labeled data. In addition, scene changes caused by changes in seasons and ground coverage will also cause a lot of false alarms in the originally effective model, as shown in Figure 2(b). It is a common practice to use the domain adaptation algorithm [5-8] to fine-tune the pre-trained model on the open source datasets to realize the migration of the source domain model to the target domain. Pseudo Label Algorithm [9] directly uses all pseudo labels to fine-tune the model, which is easy to cause the problem of catastrophic forgetting [10-12].

In this paper，we proposed a domain adaptation method for object detection in UAV based on semi-supervised learning[13,14]. The source domain model is obtain by pre-training RetinaNet [15] in visdrone2018[16]， and then pseudo labels are generated by directly applying the source domain model to the target domain of Ground target surveillance scene， by introducing the technique named scale-aware loss，the objects of abnormal scale are greatly suppressed during fine-tuning. Based on the principle of entropy regularization [17], the domain adaptation loss of the model is considered based on the Pseudo-Label algorithm, and the source domain model is fine-tuned and trained through pseudo-labels to find the low density in the source domain and target domain category distribution area to implement model migration.

2. Proposed Method

2.1. Semi-supervised learning of pseudo-labels

The Pseudo-Label algorithm [9] is based on the principle of entropy regularization [17], which uses the high-confidence samples in the pseudo-label as the maximum posterior estimation of the model, and reduces the inter-class by minimizing the conditional entropy of the class probability of unlabeled data density:

$$H(y \mid x') = -\frac{1}{n'}\sum_{m=1}^{n'}\sum_{i=1}^{C} P(y_i^m = 1 \mid x'^m)\log P(y_i^m = 1 \mid x'^m) \quad (1)$$

n' is the number of unlabeled samples，C is the total class amount， y_i^m is the unknown label of the mth unlabeled sample, x'^m is the input vector of mth unlabeled sample. Since entropy measures the degree of overlap between classes, the entropy minimization principle can find the low overlap area between classes to obtain a more accurate classification boundary. The following formula defines the maximized posterior distribution

$$C(\theta,\lambda)=\sum_{m=1}^{n}\log P(y^m \mid x^m;\theta)-\lambda H(y \mid x';\theta) \quad (2)$$

where n is the number of labeled data, x^m is the mth labeled sample, λ is a coefficient balancing two terms. By maximizing of the conditional log-likelihood of labeled data (the first term) with minimizing the entropy of unlabeled data (the second term), we can get the better generalization performance using unlabeled data.

The algorithm uses the results given by the source domain model on the target domain data as labels. These labels are not supervised and labeled by humans, so they are called pseudo labels. Pseudo-label learning is in the fine-tuning stage, using pseudo-label samples to perform multiple rounds of weight fine-tuning on the supervised training model on the source domain data set. The loss of the model in the adaptive learning process from the source domain to the target domain consists of two parts：

$$\begin{aligned} L_{total} &= \frac{1}{n}\sum_{m=1}^{n}\sum_{i=1}^{C}L(y_i^m, f_i^m) \\ &+\alpha(t)\frac{1}{n'}\sum_{m=1}^{n'}\sum_{i=1}^{C}L(y_i'^m, f_i'^m) \end{aligned} \quad (3)$$

The first item of the loss formulate the difference between predictions of model and labeled samples，while the second item is the difference between unlabeled samples and pseudo labels.

2.2. Domain adaptation of our method

In our method, we found that most of the noisy predictions comes from small targets, and these objects are either out of normal scale or out of scale with other class of objects.

$$\begin{aligned} L_{total} &= \frac{1}{n}\sum_{m=1}^{n}\sum_{i=1}^{C}L(y_i^m, f_i^m) \\ &+\alpha(t)\frac{1}{n'}\sum_{m=1}^{n'}\sum_{i=1}^{C}L_{scale-aware}(y_i'^m, f_i'^m) \end{aligned} \quad (4)$$

Motivated by DIOU loss [18], we proposed a scale-aware loss to maintain the relative ratio of the predicted target, while restricting the absolute scale of the target within a certain range based on the GPS information of the drone, the scale-aware loss is formulated as follow

$$\begin{aligned} L_{scale-aware} &= \lambda_1\sum_{j=1}^{C}(\rho_{ij}-\rho(b_i',b_j'))^2 \\ &+\lambda_2(area(b_i',H)-area(C_i,1)*H)^2 \end{aligned} \quad (6)$$

$L_{scale-aware}$ contains two parts, the first item is used to limit the scale ratio of b_i' to other categories of bounding-box, while $\rho(b_i',b_j')$ compute the the ratio of category i to category j，and ρ_{ij} is the scale ratio based on visdrone2018 statistics. The second item compute the area of b_i' to limit its absolute scale, H is flying-height of drone from its GPS system， C_i is the average area of category i.

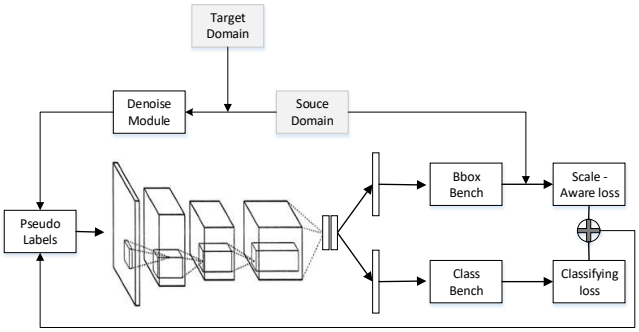


Fig.1 network architecture of our method

The proposed network architecture is shown as figure 1, the scale-aware loss is introduced during computing the loss of bounding-box predicting bench. And a denoised module based on the same principle as scale-aware loss is adapted to furtherly suppress false alarm noise.

3. Experiments

3.1. Datasets and evaluation indicators

We use the Visdrone2018 datasets for pre-training (source domain data). The data set mainly shoots scenes of streets, communities, parking lots, etc. It contains 10 categories and more than 340,000 targets. After training, it can be used in retinanet. Get a model that performs well. The target domain data is self-labeled UAV side patrol data, including 5 categories: person, car, horse, sheep, and animal, with a total of 11495 objects.

Result evaluation uses two indicators: mAP and

Average Recall (AR)，similar to the evaluation protocol in MS COCO[19].

3.2. Implement detail

All experiments are done on an RTX Titan, the selected target detection network is RetinaNet，which implemented by mmdetection [20].In the pre-training phase, the model is trained using the SGD optimizer, in the first 500 iter, we use warmup method to adjust the learning rate, from 0.001 to 0.01. In epochs 7 and 15, the learning rate is set to 0.2 times the previous. In the fine-tuning stage, the model fine-tunes 10 epochs with a learning rate of 0.001.

3.3. Domain adaption of semi-supervised learning

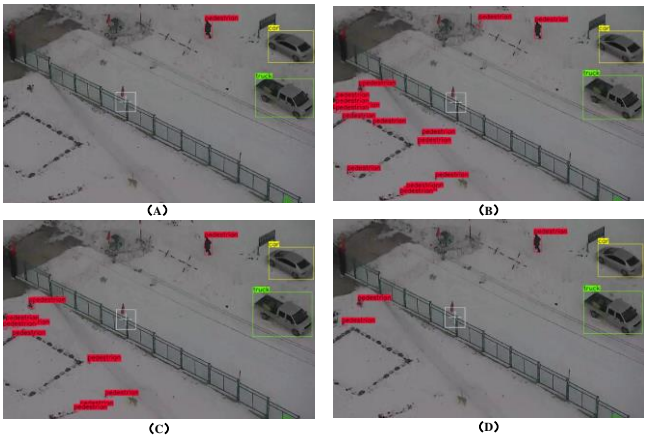


Fig.2 (a) Ground Truth; (b) False Alarms when directly applying the pre-trained model to other scence; (c) directly domain adaption without denoising; (d) our domain adption method based on semi-supervised scale-aware loss

The red bouding-box is the pedestrian target, the green is the truck, and the yellow is the car. Figure 2(a) shows the real labels of the three targets. However, in Figure 2(b), the pre-training model generates a lot of pedestrian noise in the snow scene.

After using these prediction results as pseudo-labels for model fine-tuning, the result is shown in Figure 2(c), only a small part of false alarms are suppressed. Figure 2 (d) is the result after the introduction of scale-aware loss for fine-tuning, most of false alarms are suppressed.

The proposed scale-aware loss is based on the statistics of Visdrone2018，as shown in Table 1.

Table 1 the statistics of categoried and objects of Visdrone2018-det-train datasets

Visdrone2018-det-train				
class	**num**	**Prop (%)**	**avg_H (pixel)**	**avg_W (pixel)**
pedestrian	79338	23.12	30.73	16.21
people	27059	7.88	24.7	16.41
bicycle	10480	3.05	31.21	29.46
car	144865	42.21	40.61	51.26
van	24956	7.27	47.53	54.33
truck	12875	3.75	60.72	67.73
tricycle	4812	1.4	40.41	45.09
aw-tricycle	3246	0.95	45.05	45.27
bus	5926	1.73	65.63	67.07
motor	29647	8.64	27.72	26.64

In Bianxun datasets, we apply the RetinaNet pretrained in Visdrone2018 to get the initial pseudo labels, we counted the number of denoised pseudo-labels after 10 epochs of semi-supervised training, the results are shown in Table 2.

Table 2 the number of pseudos labeled objects in diferent datasets phase before and after semi-surpervised denosing

Phase	**inital**	**denoised**	**propotion**
Train	344519	182503	52.973%
Test	71685	33287	46.435%
Valid	71500	35121	49.120%

In order to compare the effect of Pseudo-Label algorithm (PL) under different sample conditions, we use unsupervised (directly fine-tune the model with original pseudo-labels), fully supervised, and semi-supervised (our method) to fine-tune the model.We compare the results of different ways of domain adaption, as shown in Table 3.

The way of directly fine-tuning the model with original pseudo-labels cause a huge drop compared to other ways, this shows that the model has been disastrously forgotten.

Table 3 the number of pseudos labeled objects in diferent datasets phase before and after semi-surpervised denosing

Method	**AP**	**AP50**	**AP75**	**AR**
Without PL[9]	0.7	1.6	0.5	5.4
Directly PL	3.3	12.0	0.9	23.5
Supervised fine-tuning[8]	9.4	24.9	5.9	41.9
Ours	6.3	19.9	1.7	30.6

Among the various indicators of AP, AP50, AP75, AR, our method has a significant improvement compared with direct fine-tuning, which improved by 90.9%, 65.8%, 88.9%, 30.2%. Fully supervised domain adaption using manual annotation，among the indicators of AP, AP50, AR, only improved by 49.2%, 25.1%, 36.9%, which means that our method greatly improves the performance of model fine-tuning using pseudo-labels. At the same time, on some indicators, our semi-supervised domain adaptation method

achieves 70% performance under fully-supervised conditions.

4. Conclusions

Directly applying a pre-trained model from source domain to target domain can cause a lot of false alarms noise. The proposed domain adaption method which introduces scale-aware loss while model fine-tuning can greatly surpress such noise.

Experiments on the ground target monitoring data set show that the proposed semi-supervised domain adaptation algorithm achieves similar results to the supervised domain adaptation, making it possible to quickly migrate semi-supervised models. Since the scale information is used to remove a large number of false alarms, the catastrophic forgetting of the model caused by the direct domain adaptation method is avoided, which improved the detection performance of the target detection model in different environments.

Acknowledgements

This work is supported by the Foundation of Sichuan Major Science and Technology Special Project (Grant No.2018GZDZX0017)

References

[1] Krizhevsky A, Sutskever I, Hinton G E. Imagenet classification with deep convolutional neural networks[J]. Communications of the ACM, 2017, 60(6): 84-90.

[2] Xu L, Ren J S, Liu C, et al. Deep convolutional neural network for image deconvolution[J]. Advances in neural information processing systems, 2014, 27: 1790-1798.

[3] Bochkovskiy A, Wang C Y, Liao H Y M. YOLOv4: Optimal Speed and Accuracy of Object Detection[J]. arXiv preprint arXiv:2004.10934, 2020.

[4] Tan M, Pang R, Le Q V. Efficientdet: Scalable and efficient object detection[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2020: 10781-10790.

[5] Tzeng E, Hoffman J, Saenko K, et al. Adversarial discriminative domain adaptation[C]//Proceedings of the IEEE conference on computer vision and pattern recognition. 2017: 7167-7176.

[6] Daumé III H. Frustratingly easy domain adaptation[J]. arXiv preprint arXiv:0907.1815, 2009.

[7] Hoffman J, Tzeng E, Park T, et al. Cycada: Cycle-consistent adversarial domain adaptation[C]//International conference on machine learning. PMLR, 2018: 1989-1998.

[8] Ben-David S, Blitzer J, Crammer K, et al. Analysis of representations for domain adaptation[J]. Advances in neural information processing systems, 2006, 19: 137-144.

[9] Lee D H. Pseudo-label: The simple and efficient semi-supervised learning method for deep neural networks[C]//Workshop on challenges in representation learning, ICML. 2013, 3(2).

[10] French R M. Catastrophic forgetting in connectionist networks[J]. Trends in cognitive sciences, 1999, 3(4): 128-135.

[11] Kemker R, McClure M, Abitino A, et al. Measuring catastrophic forgetting in neural networks[J]. arXiv preprint arXiv:1708.02072, 2017.

[12] Kirkpatrick J, Pascanu R, Rabinowitz N, et al. Overcoming catastrophic forgetting in neural networks[J]. Proceedings of the national academy of sciences, 2017, 114(13): 3521-3526.

[13] Zhu X, Goldberg A B. Introduction to semi-supervised learning[J]. Synthesis lectures on artificial intelligence and machine learning, 2009, 3(1): 1-130.

[14] Zhu X J. Semi-supervised learning literature survey[R]. University of Wisconsin-Madison Department of Computer Sciences, 2005.

[15] Lin T Y, Goyal P, Girshick R, et al. Focal loss for dense object detection[C]//Proceedings of the IEEE international conference on computer vision. 2017: 2980-2988.

[16] Zhu P, Wen L, Du D, et al. Visdrone-det2018: The vision meets drone object detection in image challenge results[C]//Proceedings of the European Conference on Computer Vision (ECCV). 2018: 0-0.

[17] Grandvalet Y, Bengio Y. Entropy Regularization[J]. 2006.

[18] Yuan D, Chang X, He Z. Accurate Bounding-box Regression with Distance-IoU Loss for Visual Tracking[J]. arXiv preprint arXiv:2007.01864, 2020.

[19] T. Lin, M. Maire, S. J. Belongie, J. Hays, P. Perona, D. Ramanan, P. Dollar, and C. L. Zitnick, “Microsoft COCO: common objects in context,” in Proceedings of European Conference on Computer Vision, 2014, pp. 740–755

[20] Chen K, Wang J, Pang J, et al. Mmdetection: Open mmlab detection toolbox and benchmark[J]. arXiv preprint arXiv:1906.07155, 2019.

DRUG PROPAGATION PREDICTION MODEL BASED ON CA-SIS AND SVM

YUAN GAO[1], JIAN PING LI[1], FEI XIAO[1], YUE ZHOU[1]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
E-MAIL: 202021080403@std.uestc.edu.cn, jpl2222@uestc.edu.cn, 18398098564@163.com, 1026403954@qq.com

Abstract:

In recent years, opioids have been widely used in the field of analgesia treatment, and they are irreplaceable in some aspects. However, when opioids are effective, they can suppress the human immune system to some extent and are addictive. The overuse of opioids will seriously affect our social stability.

In the behavior of transmission model, the dynamic model of many nodes are based on average method, the differential equation based on the mean field theory to analyze propagation behavior, it is difficult to reflect the status and evolution of each node in the network situation, cellular automata can effectively solve this problem, so we use cellular automata as a simulation system, transmission rules, based on the SIS model combining both drug state propagation prediction model is established.

Considering that the traditional SIS model is unable to evaluate the degree of propagation (the number of drug propagation) of each node, we used the Support Vector Regression (SVR) model to predict the number of propagation of each node in the network. SVR model has the ability to deal with nonlinear multi-dimensional small samples, which has a good effect on the nonlinear regression prediction of time series, and provides a new choice for the prediction of opioid prevalence.

Keywords:

Cellular Automata; Susceptible-Infected-Susceptible; Support Vector Regression Machine

1. Introduction

In recent years, the analysis of transmission dynamics and transmission mechanism based on network has been deepened along with the research of network theory. The research on network behavior not only focuses on the dynamic process of network nodes on the network, but also focuses on understanding the structural evolution of the network itself. These studies on dynamic processes have important practical application value in analyzing propagation behavior in the real world.

In real life, every individual has a certain amount of self-control. When people in a certain county or city are informed of the epidemic of opioids, local authorities or people will take adaptive measures to reduce the scale of the spread of illegal opioids, which can lead to the improvement of the situation at their own nodes. For example, some Gross et al. in the Susceptible to infection to Susceptible (Susceptible-infected- Susceptible (SIS) model [1], and Shaw et al. In their study of the Susceptible to infection – infected - Susceptible (Susceptible to infection - immune - Susceptible (SIRS)) model of adaptive networks, both of them believe that when Susceptible nodes have infected neighbors, Vulnerable nodes will take protective measures to ensure that there is a certain probability of recovery.

In the quantitative analysis of propagation simulation, the prediction of time series data is an important part, which needs to achieve the effect of simulation prediction through regression prediction of the data on the geographic network. In fact, the prediction of the temporal data is a multidimensional data regression problem. In machine learning, there are many models that can deal with linear or nonlinear regression prediction of multidimensional data, such as multi-layer perceptron, autoregressive sliding average model, support vector machine and so on.

2. Materials and methods

2.1. Data Set

Based on the number of opioid reports provided by the US Centers for Disease Control (CDC) from 2010 to 2017, 461 counties in five US states (Ohio, Kentucky, West Virginia, Virginia and Tennessee) were selected for transmission behavior analysis projections.

2.2. Opioid spread model based on Cellular Automata

In this part, we compared the transmission of opioid to the transmission of infectious diseases, and then built an SIS (Susceptible-Infected-Susceptible) contagion model based on Cellular automata (CA) to analyze the transmission characteristics of Opioids. The structure of CA is shown as below.

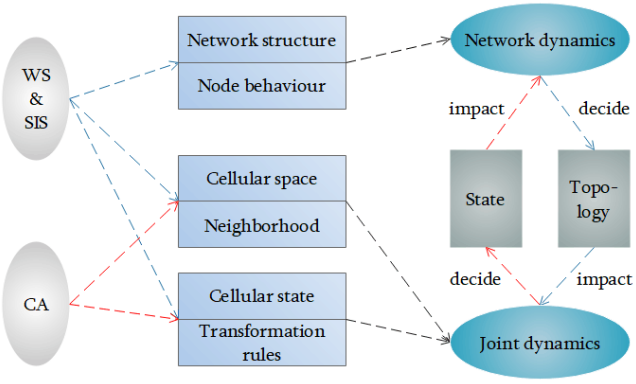


Fig.1 The structure of CA

Cellular automata (CA) is a discrete dynamical system with simple structure but complex self-organizing behavior. CA can overcome the defects of the differential equation model based on the mean field method. It is an effective alternative method to study complex systems and their dynamics. The existing research shows that CA has its inherent advantages in reflecting the interaction between individuals, the expression of network topology, the spatial characteristics of nodes and the description of probability events in the process of propagation [2].

In this article, we set each county as a node and utilize the connections between nodes to form a WS small-world network. Then the node state and state change rules are defined according to the actual situation, and the rules can be divided into propagation rules and reconnection rules. The specific steps of CA construction are as follows:

Step 1. Define the following quaternion to describe the CA:

$$A = (C, Q, V, f) \tag{1}$$

where A is the CA system, C is the Cellular space, Q is the finite state set of cellular, V is the cellular domain, f is the cellular state transition rule function.

Step 2. Define the evolution rule of f, which can be expressed as:

$$Q_i^{t+1} = f(Q_{j1}^t, Q_{j2}^t, \dots, Q_{jN}^t) \tag{2}$$

where Q_i^{t+1} represents the state of the i_{th} cell at time t+1, $(Q_{j1}^t, Q_{j2}^t, \dots, Q_{jN}^t)$ is the set of all neighbors.

2.3. SIS spread rules

According to the SIS propagation process, any node can only be infected by its neighbor at each time step. The I state node tries to infect each of its neighbors in the S state with probability β. This process is called infection. Meanwhile, nodes in state I are restored to state S by probability δ. This process is called healing [3].

The corresponding differential equation of SIS model is as follows:

$$\begin{cases} \frac{dS(t)}{dt} = -\beta I(t)S(t) + \delta I(t) \\ \frac{dI(t)}{dt} = \beta I(t)S(t) - \delta I(t) \end{cases} \tag{3}$$

Where, I(t) is the proportion of the number of infective nodes at time t, and S(t) is the proportion of the number of susceptible nodes at time t. Since there are only susceptible states (S state) and infective states (I state) in SIS model, the result is I(t)+S(t)=1.

Connections between states and counties not only depend on fixed geographic locations, but also on the movement of people between regions. Accordingly, the network structure of each state and county is a time-varying network that changes constantly with time. To simulate population flow between regions, we introduce the rule of network reconnection.

The general method of reconnection is to disconnect one end of each selected connection and randomly connect it to other nodes, without allowing self-connection and repeated connection.

For this, we combine gravity model to optimize the reconnection rule. Use the following formula to calculate the degree of connection between any two nodes (counties).

$$T_{ij} = K_{ij} P_i^{\alpha} P_j^{\gamma} F_{ij}^{-\theta} \tag{4}$$

Where T_{ij} is the population flow; F_{ij} is the generalized distance between zone i and j (here is the actual distance); P_i, P_j the populations of the two regions; K_{ij} is the socio-economic adjustment coefficient of zone i and zone j; α, γ, θ are correction factor.

2.4. Opioid spread prediction model based on SVR and CA-SIS

The CA model mentioned above only makes qualitative analysis of opioid propagation, so quantitative analysis of the propagation process is also needed. In order to ensure the objectivity and accuracy of prediction results, we built the opioid propagation prediction model based on SVR (Support Vector Regression).

Proposed by Corinna Cortes and Vladimir Vapnik in 1995, SVM is a supervised learning model for data classification, regression analysis and outlier detection. Its advantage is that it is effective in high dimensional space, and can effectively implement the nonlinear classification case through the introduction of the nuclear mechanism. In the case of linear indivisibility, the kernel function is introduced to overcome the dimension disaster effectively. Another feature of SVM is that it minimizes the structural risk and can effectively solve the problem of local minimum and over-learning [4].

There are many subprograms in SVM. SVR, which is

one of them, has a strong non-linear processing power. This method usually combine with Time Series Forecasting to make predictions.

The specific steps of constructing SVR are as follows:

Step 1: For a given data set, construct a regression function. The calculation formula is as follows:

$$N(x) = \omega \cdot \varphi(x) + b \tag{5}$$

Where ω is weight vector, b is bias.

Step 2: Introduce insensitive loss functions ε and relaxation variables ξ , ξ_i^*. The support vector regression machine can be expressed as a quadratic programming problem. The calculation formula is as follows:

$$min\ R(\omega, b) = \frac{1}{2}||\omega||^2 + B\sum_{i=1}^{l}(\xi_i + \xi_i^*) \tag{6}$$

$$s.t.\begin{cases} y_i - \omega \cdot \varphi(x) - b \le \varepsilon + \xi_i\ ,\ \xi_i \ge 0 \\ \omega \cdot \varphi(x) + b - y_i \le \varepsilon + \xi_i\ ,\ \xi_i \ge 0 \end{cases} \tag{7}$$

where B >0, is penalty factor

Step 3: Introduced Lagrangian coefficients a_i and a_i^*, convert the above equation into a dual problem. The calculation formula is as follows:

$$max\ W = \frac{1}{2}\sum_{i=1}^{l}\sum_{j=1}^{l}(a_i - a_i^*)(a_j - a_j^*)K(x_i - x_j) - \varepsilon\sum_{i=1}^{l}(a_i + a_i^*) + \sum_{i=1}^{l} y_i(a_i - a_i^*) \tag{8}$$

$$s.t.\begin{cases} \sum_{i=1}^{l}(a_i - a_i^*) = 0 \\ B \ge a_i, a_i^* \ge 0 \end{cases} \tag{9}$$

where $K(x_i - x_j)$ is Kernel function

Step 4: The final support vector machine model function formula is as follows:

$$N(x) = \sum_{i=1}^{l}(a_i - a_i^*)\,K(x_i - x_j) + b \tag{10}$$

MAE will be used as the evaluation indicator below.

3. Experimental results analysis

3.1. Future evolution of CA-SIS

With the CA-SIS model we can estimate future opioids transmission. Thus, we evolve the opioid transmission in 2018, as shown in the figure below:

Fig.2 The evolution of Buprenorphine in 2010

Fig.3 The evolution of Buprenorphine in 2018

In this map, Fig 2 shows the 2010 levels of Buprenorphine transmission, while Fig 3 shows the predicted 2018 levels. Where 0 indicates that no such drug has been reported and 1 indicates that Buprenorphine has been found.

The changing trend reflected in the figure shows that if the United States government does not take effective measures to control the situation, the scope of influence will expand further, which may eventually lead to the abuse of opioids in the whole region.

The figure below shows the predicted and actual infection rates.

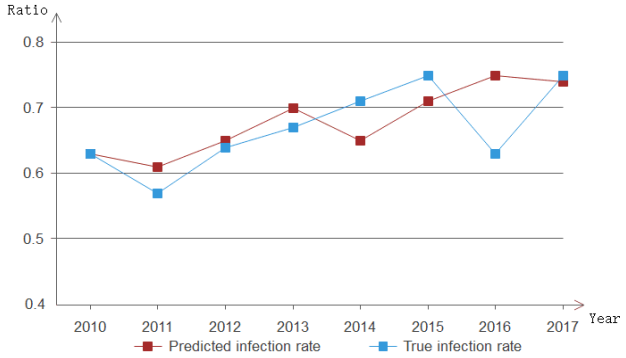


Fig.4 Graph of predicted and true infection rates

As can be seen from the figure, our predicted results match well with the actual results, which shows that our CA-SIS model has a good prediction effect.

3.2. Analysis results of propagation characteristics

Since CA can only conduct qualitative analysis on the prediction of propagation and cannot describe the characteristics of propagation in detail, we visualized the propagation by combining the SVR model in Section 2.3. Our CA-SIS is based on the Drug Reports of 2010. After evolution, the spread of opioids in 2011 and 2018 is shown below.

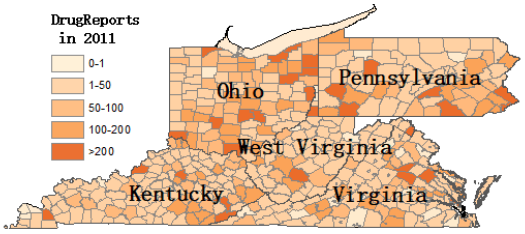


Fig.5 Predicted results of Drug Reports in 2011

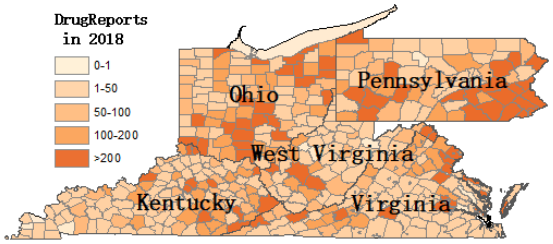


Fig.6 Predicted results of Drug Reports in 2018

Based on the SIS transmission rules, it can be observed that the spread of opioids is central, multi-source and endemic. Moreover, due to the impact of the developed transportation system on modern society, opioids have the nature of trans-regional transmission.

Upon examination, from 2011 to 2017, the state of the simulation accuracy is over 83%, the test set of the mean absolute error (MAE) is 88.8, due to some county in more than 1000 the number of drug transmission, driving up this kind of error average, so in the process of error detection, this paper is divided into three categories: the counties and cities in the number of class 1 for drug spread in 200 counties and cities, under 2 classes for drug spread the number under 200 more than 1000 counties and cities, three kinds of drug quantity in more than 1000 counties and cities. The average absolute error of category 1 is 29.8, category 2 is 103.3, and category 3 is 265.7, which is acceptable.

4. Conclusion

We study the predictive model of drug transmission based on machine learning. First of all, in the form of cellular automata, the simulation of opioid propagation based on geographic network is made. By referring to the transmission dynamics model SIS (susceptibility-infection-susceptibility model), the evolution rules in cellular automata, namely the transmission rules, were established. Based on this, the opioid transmission at a certain location could be determined, and the qualitative analysis model of opioids was completed. On this basis, the classical machine learning model support vector regression machine was used to carry out regression prediction for the time series of opioid quantity, and a certain test set was selected to verify the accuracy.

Due to the complexity of social network, the real drug transmission will be affected by many factors. This paper mainly considers geographical network, socio-economic factors, the real number of opioid transmission and other factors, but there are still insufficient considerations. Further research can be carried out from the following point:

Due to the lack of traffic flow data in the five selected states, the influence of population mobility factors was not considered in the study of this paper. When the network structure of cellular automata is further optimized, the complex network model can be considered to obtain traffic data to improve the model.

According to the model in this paper, we can not only apply to drug transmission. By adjusting the model parameters, it can also be applied to many propagation behaviors, such as public opinion propagation.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, the project of Science and Technology Department of Chongqing Municipality, Chengdu Chengdian Network Technology Co., Ltd., Chengdu Civil-military Integration Project Management Co., Ltd., and Sichuan Yin Ten Gu Technology Co., Ltd.

References

[1] Gross Thilo, Blasius Bernd. Adaptive coevolutionary networks: a review[J]. Journal of the Royal Society, Interface,2008,5(20).

[2] T. Soemsap, S. Wongthanavasu and W. Satimai, "Forecasting number of dengue patients using cellular automata model," 2014 International Electrical Engineering Congress (iEECON), Chonburi, 2014, pp. 1-4, doi: 10.1109/iEECON.2014.6925876.

[3] G. Li, D. Shi and Z. Zhang, "The Discrete-Time SIS Model in Small-World Networks," 2012 International Conference on Computer Science and Service System, Nanjing, 2012, pp. 1378-1380, doi: 10.1109/CSSS.2012.347.

[4] Y. Dong, W. Cheng and S. Li, "A new regression method based on SVM classification," 2011 Eighth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Shanghai, 2011, pp. 770-773, doi: 10.1109/FSKD.2011.6019663.

BEHAVIORAL BIOMETRICS FOR HUMAN IDENTITY CORROBORATION BASED ON GESTURE-SIGNATURE WITH DEEP LEARNING

EDWARD OPOKU-MENSAH[1,2,*], YAA SERWAA BANDOH[2], LI JIANPING[1], JUDITH BROWNE AYEKAI[1] , BERNARD COBBINAH MAWULI[1]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu Sichuan, China
[2]Department of Computer Science, Christian Service University College, Ashanti Region, Ghana
E-MAIL: edwardopm@ieee.org, yaasbe@gmail.com, jpli2222@uestc.edu.cn, ayekaibrowne@hotmail.com, cobbinahbernard@ieee.org

Abstract:

Identity corroboration has gained a substantial deal of attention with the high usage of smart devices and dedicated systems accommodating sensitive data and applications magnitudes. In this paper, we develop a behavioral biometric authentication system based on deep learning. Specifically, an android application is developed as a dedicated tool for capturing the touch behavioral biometrics information, the electronic signature information alongside their corresponding accelerometer and gyroscope sensor readings. Finally, the generated sensor readings are fed into a multi-input convolutional neural network architecture for classification. Extensive experimental results show that our proposed approach uniquely identifies users with a classification performance of 93.46% as compared to other baseline approaches, where only a single sensor reading is considered.

Keywords:

Behavioral biometrics; Human identity corroboration; Smartphones; Multi-input Convolutional neural networks.

1. Introduction

In recent digital authentication researches, biometric authentication has increasingly become a research hotspot. The primary objective of biometric authentication is the automated verification of a living person's identity by proving over some unique feature that only the person possesses. However, non-biometric authentication is not based on an individual's inherent attributes, which exposes some challenges of a weak authentication method and poor experience vulnerable to external malicious attacks to solve security issues for user authentication within mobile phones.

One type of biometric authentication is physiological-oriented such as fingerprint, retina, iris, the geometry of face, ear, hand, etc. This is generally called 'static modality' because, supposedly, these biological properties do change very little or not at all over time. Moreover, these static biometric features are grounded from stationary body surfaces, be it an image of hand palm or the pattern of vascular veins, tissues on a hand, or face. However, the static biometric features alone do not guarantee safety from unauthorized users, raise privacy concerns, and are convenient only for limited applications since the system becomes very slow for a large number of users.

Fig.1 Behavioral biometric features for the proposed framework.

More profoundly, behavioral biometrics, which is apparent in a person's interaction with the environment, such as signatures, gaits, and keystroke, are more likely to ensure a robust digital authentication system because it both defines a person and provide unique features. However, due to pressing security reasons, it is always desirable to enhance the robustness of behavioral biometrics signature acquisition systems by other means using digital sensor readings of gyroscope and accelerometer.

This paper proposes a new concept for behavioral biometric authentication using deep learning on digital sensory gesture-signatures from gyroscope and accelerometer readings. The contributions of this work are:

- A deep multi-input convolutional neural network architecture for behavioral biometric authentication.
- The authentication is based on the electronic signature information alongside their corresponding accelerometer and gyroscope sensor readings.
- The performance of our proposed biometric

authentication approach is empirically validated and reports promising results.

- A new graphical user interface for behavioral biometric user authentication.

2. Related Work

Passwords, PINs, and Patten as entry methods for user credential corroboration have been enormous in both computer technologies and mobile devices and/or applications. This paper's primary purpose is established on the innovative enhancement of traditional entry methods, which has led to various researchers' questing into this context.

2.1. Touch Behavioral Biometrics and Keystrokes

According to findings in [2] Keystroke dynamics have been predominantly targeted by researchers to establish the validity of users. Research has been conducted to explore and discover diverse techniques to make available addition layers of safeguards to protect client credentials' integrity and accessibility for accessing their devices, etc.

Another method or scheme that possesses its pros and cons [3], took the interest of other researchers to delve into is the graphical password schemes [4].

According to [5], the typing nature or pattern of online users as they browse can be reassembled and used to detect a user. This information, together with [6], which talks about how operators of telegraphs exhibit individualistic typing regularity, clearly indicates that individual users have peculiar behaviors in keying or typing habits.

2.2. Accelerometer and Gyroscope sensors.

According to [7], sensing and reacting based on an environment is a vital goal and role in mobile computing. In referring to Android documents for detailed descriptions of available sensors [8], it can be identified that various kind of embedded sensors such as Accelerometer, Barometer, Gravity sensor, Gyroscope, Light sensor, Magnetometer, Proximity sensor, Humidity sensor, and the like are available on these mobile devices. These sensors are now a very rich source of data to measure a user's daily life's numerous characteristics. As a result, smartphones and devices are rising rapidly to be an excellent source for human activity recognition.

2.3. eSignature Dynamics

In accordance to the United States Federal ESIGN Act [10], and the United States legislation & Electronic Signature & Records Association (ESRA) [11], an electronic signature is "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record" [12].

Its simplest form can be described as an electronic expression of a signatory's agreement to a set term of a particular deed. The versatile nature of its definition with the inclusion of process, sound or symbol raises the opportunity for potential vendors as AssureSign to provide a beneficial number of solutions with the power to capture electronic signatures [12].

2.4. Deep Learning on Biometric Recognition

Using deep learning for biometric recognition, one can learn a hierarchy of concepts as we go deeper into the network. Xin et al. [13] proposed a palmprint recognition using a deep learning framework. The authors designed a deep neural network using unsupervised training and fine-tuned the model parameters toward a robust accuracy on the test set. Zhang et al. [14] proposed a hybrid classifier in conjunction with a DC-GAN network to learn to extract the signature features in an unsupervised manner. In another work [1], they proposed an iris recognition network based on a convolutional neural network, which provides a, discriminative model, resulting in a very high accuracy rate, in cross-sensor recognition of iris images. Zhang et al. [15] also proposed a Siamese neural network for gait recognition, where the sequences of images are converted into gait energy images.

3. Proposed Approach

Aforementioned, the objective of this current work is to use gesture-based signatures alongside their corresponding accelerometer and gyroscope sensor readings to design a behavioral biometric authentication using a multi-input convolutional neural network. The entire methodology involves three stages: Accelerometer sensor readings, electronic signature behavioral data capturing, and the Multi-input fusion convolutional neural network architecture.

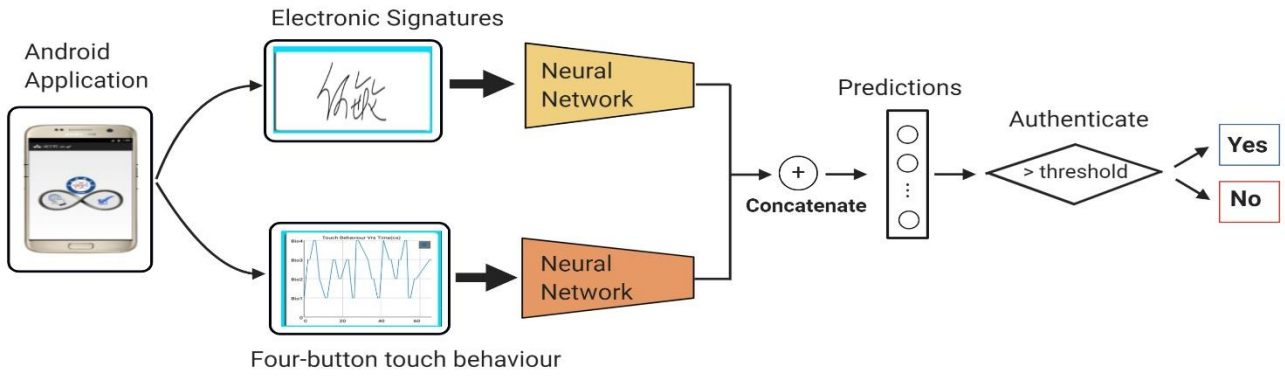


Fig.2 Behavioral biometric authentication proposed framework.

For the extraction of behavioral data, user pattern information will be established via the Android MotionEvents, GestureListener, onTouchListener, among others. With the aid of features embedded in Android devices such as Accelerometer, gyroscope, Barometer, Gravity sensor and Magnetometer, very precise information may be obtained and implemented to richly enhance the overall significance and robust performance of this work.

Research works from a number of related researchers had to rely on 3rd party applications that were not overall specific to their needs, with others even having to combine different apps to capture different aspects of their research on varying apps, one at a time with the same user. In this work, we develop our own user interface application tailored towards the capturing of the electronic signatures and the sensor readings for the purpose of this current paper. The general framework of this paper is showed in Figure 2.

3.1. Touch Behavioral Biometric Sequence Graph Generation

This section involves the first part of the user touch biometrical behavior recording session, by how the user interacts with four infinite touch buttons. They are programmed to handle an infinite number of touch behavioral sequence as desired by the user. The accelerometer sensor readings are initiated once any of the available options are touched. Specifically, a four-button user interface is provided in the form of an android graphical user interface. As the user interacts with these buttons in the form of a chosen pattern, a graph is generated using the recorded sensor readings with respect to time. Each user is made to repeat the whole process one hundred and fifty (150) times to generate more accelerometer pattern graphs for a fair model. All 150 repetitions (for each participant) were captured from 4 different sessions in 9 days.

It should be noted that for all referencing and session tracking, accelerometer readings are sensed and recognized as behavioral data as individuals interact with the application. They are rendered in Unicode Transformation Format using 8-bit blocks to represent a character (UTF-8) mode, for display.

Alg.1 Accelerometer Sensor Reading

Precondition: Android hardware library, SensorEvent, SensorManager, SensorEventListener
Input: isRunning, fileWriter, captureNo =150: Number of session instances
Output: sensorGraphs: Accelerometer pattern graphs
1: **if** AllPreconditionsSatisfied **then**
2: *isRunning* ← startApp();
3: **if** *isRunning* == *True* **then**
4: **for** n ←= 1 to *captureNo* **do**;
5: SensorManager.registerListener();
6: **while** patternInteraction **do**;
7: SensorManager.registerListener();
8: *spikeTime*← $getCurrentTime()$;
9: sensorReading ← startAccelerometerReading( );
10: sensorGraph ← fileWriter.*generateGraph* (*spikeTime,* sensorReading);
11: sensorGraph*s* ← sensorGraph.insert()
12: **endwhile**
13: **endfor**
14: **endif**
15: **endif**
16: **return** sensorGraphs;

3.2. Electronic Signature Behavioral Data Capturing

After capturing the user touch patterns with the accelerometer readings, an electronic signature is also

captured with a different user interface in the same app. The captured electronic signature behavioral information section is involved in the mannerism in which user interacts with the provided signing pad section. They are programmed to handle an infinite number of signature stroke sequence as desired by the user. But in this work, each user has a five hundred signature signing session.

Gyroscope sensor readings are initiated once any sign pad is touched (when touch behavior readings commence).

Alg.2 Gyro Sensor eSignature Reading

Precondition: Android hardware library, *SensorEvent*, SensorManager, SensorEventListener
Input*:* firstSession: flag to check if first stage is completed, fileWriter, eInstances = 150: Number of session instances.
Output: eSignature: Electronic signatures,

```
1:  if firstSession == True then
2:    for n ←= 1 to eInstances do;
3:      SensorManager.invokeGyroscope();
4:      while signatureStrokes do;
5:        SensorManager.registerSensorChange();
6:        strokeTime← getCurrentTime();
7:        gyroReading ← startStrokeReading();
8:        eSignature ← convertToImage(gyroReading)
9:        fileWriter.saveSignature(eSignatue)
10:     endwhile
11:   endfor
12:  endif
13: endif
```

Each background information is cumulatively recorded, converted, and saved in both seconds and microseconds in all sensor readings. It is used as the baseline for graph limit rendering. Hence, it is activated on first touch instance recording when a touch or click event listener is triggered and deactivated on a successful commit request.

3.3. Multi-Input Convolutional Neural Network (CNN)

We implemented a convolutional siamese network (CSN) upon the raw captured accelerometer reading graph and the gyroscope sensors' electronic signatures. Siamese networks are comprised of twin neural networks that learn to predict whether or not a pair of input images are similar or dissimilar. Pairs of each data were fed into the CSN and the convolutional sub-networks of the CSN learned to produce representative feature vectors of each case for the behavioral biometric authentication.

Our siamese network exploits a standard CNN as the base network. Each of the twin networks has convolutional network layers, batch normalization, and max-pooling as its base. Specifically, the base CNN model utilized for twin networks has four convolutional layers channel with filters of sizes 16, 32, 64, and 64 feature maps, respectively. Each convolutional layer operates on a stride of 1 and a kernel size of 3 × 3. Each convolutional layer is followed by a batch normalization layer and a max-pooling layer of 2×2, operating at a stride of 1. All convolutional layers in our base CNN have Rectified Linear Units (ReLU). The output of each of the twin network's final max pool layer is flattened into a vector, concatenated, and fed into the succeeding fully connected dense layer having 512 hidden units, followed a dropout layer of value 0.5 and finally 50 sigmoid units representing the class probabilities.

Each network's model parameters (weight and biases) are shared by both individual twin networks, resulting in fewer learning parameters. Consequently, Siamese Networks require relatively fewer data to train and are less susceptible to overfitting. We trained the siamese network for 150 epochs with a learning rate of 0.0001. For training the siamese network architecture, the categorical cross-entropy loss L_c function is used. The cross-entropy function measures a classification model's performance whose output is a probability value between 0 and 1. Cross-entropy loss increases as the predicted output diverge from the actual class. For this task, the cross-entropy loss is calculated as:

$$L_c = -\sum_{c=1}^{M} y_i \log(p_i) \quad (1)$$

Where M is the number of classes (users), y_i and p_i is the binary target indicator and predicted class probability of observation i, respectively.

We tested that the network had learned feature vectors representing the original cases by comparing this to a threshold to identify whether a pair of examples belonged to the same class (a genuine pair) or different classes (an impostor pair). If we determined that the classification probability is above a set threshold, then a real pair and an impostor pair are less than the threshold. We reasonably assume that the network has authenticated a user if after mapping an input pair to a user and has its confidence probability above the specified threshold. We, therefore, used the percentage of correctly identified pairs as our accuracy metric.

4. Experiment

This section empirically evaluates the efficiency and effectiveness of our proposed multi-input convolutional behavioral biometric authentication system. We compared the multi-input proposed method with two approaches:

(1) **Captured accelerometer pattern graphs (CAP)**: A single base of the siamese convolutional neural network is used to train on the captured accelerometer reading of the four-button user interface.

(2) **Electronic signatures (ES)**: The same single base of the siamese convolutional neural network is trained on the captured electronic signatures.

4.1. Dataset

We collected real-world dataset from 50 individuals from different university campuses using our android graphical user interface application to conduct our experimentation. Each sensor reading captured as described in section 3.1 and 3.2, each individual generated 150 sample pair for both the accelerometer graph and the electronic signatures. In total, 7500 image pairs (input) were used as the dataset, which are randomly divided into a group of 6000 and 1500; for training, and test sets, respectively. We applied data augmentation to increase diversity in the training data sample pairs and make our model more robust. We applied Gaussian blur with sigma value ranging between 0 and 1.3, both vertical and horizontal flip, with a probability of 0.5, and image rotation between the angle of -45 and 45. We produced an increasing amount of training dataset for each user with the formulae.

$$T_c = n_c \times K \tag{2}$$

Where T_c is the new amount of dataset for each individual c, n_c is the initial number of each class before data augmentation, $K = 2$ is the increment factor and $c \epsilon \{1,2, \dots 50\}$. After the augmentation, total number of training dataset pair becomes 12000.

Each image is assigned a label from the 50 categories representing the number of individuals. For all the experiments, the resolution of both input pair images was set to 250×235 with an input channel of 3. All datasets were normalized between 0 and 1 with the formulae:

$$A_{norm(i,j)} = \frac{a_{(i,j)} - mean(a_j)}{std(a_j)} \tag{3}$$

where a_j is the jth column of the matrix (A).

4.2. eSignature Exposition

The captured electronic signature is accompanied with associated attributes. The gyroscope sensor is initiated once the sign pad receives a touch event and ends when user commits. The application user interface is programmed to be both assistive and user friendly. Due to this, participants are given the opportunity to save a successful session to commit, or discard a session that experienced an extremely unusual occurrence.

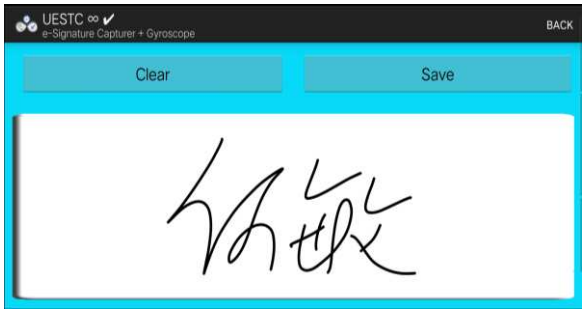


Fig.4 Captured signature session

4.3. Behavioral graph exposition

The graph exploration on the four-button display showed an identifiably distinct representation based on the individual participants interacting and exhibiting their traits while interacting with the application.

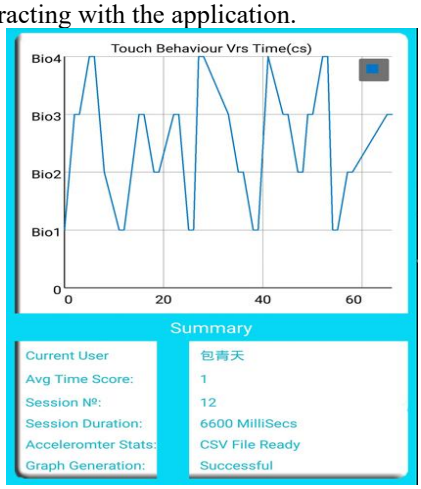


Fig.3 Results from Touch behavioral biometrics captured.

4.4. Network Architecture

The siamese network was optimized using Adam optimizer and the hyperparameters in Table 1. The output of the concatenated sub-networks was a predicted 50-unit softmax probability. To be comparable with the two baseline approaches, we maintained one of the single base networks of the siamese network for comparison purposes as a close replica of one of the sub-networks. Implementations were run for 150 epochs as the loss had reached a sufficiently low value by this point. Experiments were repeated ten times and a mean percentage of accuracy calculated using a probability threshold of 0.7 for the test set.

Table 1 Network hyperparameter settings.

Hyperparameter	Value
Learning Rate	0.0001
Epoch	150
Dropout	0.5

4.5. Evaluation Metric

In this work, 80% of the dataset's sample pairs were used for training and 20% for testing. The performance of our approach is evaluated with the accuracy metric defined as

$$Acc = \frac{(TP+TN)}{(TP+TN+FN+FP)} \quad (4)$$

. Specifically, if a user A is classified as A, this is deemed as a TP and otherwise as FN. Also, TN denotes the number of users truly classified not to be the users, and FP denotes the number of users classified to be the users but are not. It should be noted if a user A is classified as A but the classification probability is less than the confidence threshold (0.7), it is a FP. This is because in a security authenticating system, access guarantee with high confidence is of maximum priority.

4.6. Classification results

We evaluate the performance of our proposed method, together with the two baseline approaches. For each approach, we report the classification accuracy for the scenario where the threshold confidence (0.70) is considered and when there is no threshold (0). We are more interested in the case where the threshold is set because it makes more intuitive sense to authenticate users with high confidence than allowing unauthorized users to access a security authenticating system. We report our results in Table 2.

Table 2 Test prédiction accuracy of all approaches.

Approach	Test Accuracy (%) with no threshold	Test Accuracy (%) with threshold
ES	99.81	90.15
CAP	97.92	89.73
Multi-input	98.69	93.46

ES = Electronic signatures convolutional neural network; CAP = Captured accelerometer pattern graphs with convolutional neural network; Multi-input = Multi input behavioral biometric convolutional neural network.

It could be deduced from Table 2 that the performance of the multi-input behavioral biometric authentication approach performed better than the other baseline approaches when a threshold confidence is set. Though the ES approach recorded a greater classification accuracy than the Multi-input when there is no threshold, it does not guarantee a higher confidence of the system authenticating the right user. The multi-input behavioral biometric convolutional neural network shows a high integrity performance and accurately validates a user before authentication.

5. Conclusions

This paper introduces a behavioral biometric authentication system using gesture-based signatures alongside their corresponding accelerometer and gyroscope sensor readings. The sensor readings are fed as a multi-input pair into a deep convolutional neural network for classification. We compared the proposed approach with single sensor readings classification performance for scenarios with and without a set threshold.

Experimental results (ES=90.15%, CAP=89.73% and Multi-input=93.46%) prove that the multi-input behavioral biometric authentication approach shows more robust performance as it has a high capability of uniquely identifying users' behavioral patterns and making it more secured. Together, the two sensor input pairs make up for each other's disadvantage in the real-life scenario. Our prime idea focused on by this research dwells upon the benefits of the input merger for a behavioral biometric authentication system.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, the project of Science and Technology Department of Chongqing Municipality, Chengdu Chengdian Network Technology Co., Ltd., Chengdu Civil-military Integration Project Management Co., Ltd., and Sichuan Yin Ten Gu Technology Co., Ltd., the Computer Science and Information Technology departments of Christian Service University College, University of Electronic Science and Technology of China, and two IEEE Young Professionals & Computational Intelligence society members.

Profound appreciation to Huawei Technologies SA Ghana for the enlightenment during the 1-year work and study experience.

References

[1] Abhishek Gangwar and Akanksha Joshi. Deepirisnet: Deep iris representation with applications in iris recognition and cross-sensor iris recognition. In 2016 IEEE International Conference on Image Processing (ICIP), pages 2301–2305. IEEE, 2016.

[2] M. Nauman, T. Ali, and A. Rauf, "Using trusted computing for privacy preserving keystroke-based authentication in smartphones," Telecommun. Syst., vol. 52, no. 4, pp. 2149–2161, Apr. 2013, doi: 10.1007/s11235-011-9538-9.

[3] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely Automated Attacks on PassPoints-Style Graphical Passwords," IEEE Trans. Inf. Forensics Secur., vol. 5, no. 3, pp. 393–405, Sep. 2010, doi: 10.1109/TIFS.2010.2053706.

[4] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical Passwords: Learning from the First Twelve Years," ACM Comput. Surv., vol. 44, no. 4, p. pages 19:1--19:41, 2012, doi: 10.1145/2333112.2333114.

[5] P. Chairunnanda, N. Pham, and U. Hengartner, "Privacy: Gone with the typing! Identifying web users by their typing patterns," Proc. - 2011 IEEE Int. Conf. Privacy, Secur. Risk Trust IEEE Int. Conf. Soc. Comput. PASSAT/SocialCom 2011, pp. 974–980, 2011, doi: 10.1109/PASSAT/SocialCom.2011.197.

[6] W. L. Bryan and N. Harter, "Studies in the physiology and psychology of the telegraphic language," Psychol. Rev., vol. 4, no. 1, pp. 27–53, 1897, doi: 10.1037/h0073806.

[7] M. Roccetti, A. Semeraro, and G. Marfia, "On the design and player satisfaction evaluation of an immersive gestural game," in Proceedings of the 29th ACM international conference on Design of communication - SIGDOC '11, 2011, p. 45, doi: 10.1145/2038476.2038485.

[8] "Sensors Overview | Android Developers." https://developer.android.com/guide/topics/sensors/sensors_overview (accessed Feb. 19, 2019).

[9] Summary: Bills Pertaining to Digital Signatures and Authentication in the 106th Congress. .

[10] "ESRAHome | ESRA." https://esignrecords.org/ (accessed Mar. 10, 2019).

[11] "HelloSign's Guide to Electronic Signatures." https://www.hellosign.com/electronic-signature (accessed Jan. 30, 2019).

[12] "What Is Electronic Signature?" https://www.assuresign.com/what-is-electronic-signature/ (accessed Mar. 19, 2019).

[13] Zhao Dandan Pan Xin, Pan Xin, Luo Xiaoling, and Gao Xiaojing. Palmprint recognition based on deep learning. 2015

[14] Zehua Zhang, Xiangqian Liu, and Yan Cui. Multi-phase offline signature verification system using deep convolutional generative adversarial networks. In 2016 9th international Symposium on Computational Intelligence and Design, volume 2, pages 103–107. IEEE, 2016.

[15] Cheng Zhang, Wu Liu, Huadong Ma, and Huiyuan Fu. Siamese neural network based gait recognition for human identification. In International Conference on Acoustics, Speech and Signal Processing. IEEE, 2016.

QCS-CNN: A NEURAL NETWORK OPTIMIZATION ALGORITHM IN RESOURCE-CONSTRAINED ENVIRONMENT

DI LIU[1], ZHIZHAO FENG[1]

School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China
E-MAIL: liudi@uestc.edu.cn fengzhizhao@std.uestc.edu.cn

Abstract:

Due to the complex models and large amount of calculation, deep neural networks cannot be deployed on resource-constrained devices. In order to apply deep neural networks to resource-constrained devices, this paper proposes a QCS-CNN neural network optimization algorithm. It can compress the input image, while reducing the number of parameters, it can quantize the precision of all parameters in the network from 32 bits to 8 bits. The experiments on MNIST data set show that QCS-CNN neural network optimization algorithm can effectively reduce the amount of calculation and accelerate the inference speed of the model.

Keywords:

Resource constraint; Neural network; Model optimization; Network quantification

1. Introduction

In recent years, with the substantial improvement of computer hardware capabilities, deep neural networks have received more and more attention. With the continuous increase of the depth of the network layer, the learning ability of deep neural network is also enhanced. Deep neural networks are used in many fields, such as computer vision [1- 6], natural language processing (NLP) [7] and speech recognition [8]. Complex models certainly have better performance. However, due to its large amount of computations and high storage cost, for example, VGG16 has more than 130 million parameters, making it difficult to use on resource-constrained equipment. Therefore, under the condition of ensuring the accuracy of the model, accelerating the inference speed of the network model has become an urgent problem to be solved.

At present, many researchers are studying how to compress and accelerate neural networks. The main methods are quantization network pruning [9-10], network weight decomposition [11-12] and knowledge extraction [13].

SHEN et al. proposed a new network architecture CS-CNN[14], which can significantly reduce the number of parameters in the input layer and accelerate the inference speed of the model. Because of the deep neural network has many layers, but CS-CNN only considers the input layer and does not process the data in the middle layer, resulting in limited acceleration effects. This paper introduces network quantification on this basis. Quantization is to approximate the weights and biases represented by floating-point numbers (high-precision) with low-precision integers (usually INT8). In this paper, the 32 bits floating point is quantified to 8 bits, which can effectively reduce the parameter of the entire network and speed up the inference speed of the model.

The main contributions of this paper are:

1) Analyzed and studied the performance bottlenecks in deep neural networks and the current solutions.
2) The CS-CNN model is optimized, and the network quantization is introduced to process the middle layer of the network, which speeds up the inference speed of the model. And named it QCS-CNN.

2. Related Work

Quantization and pruning are effective methods to speed up model inference and reduce model size.

Network pruning is to reduce a large number of parameters by removing some unimportant parameters from the trained network. Through continuous pruning and retraining, it can be ensured that the accuracy is not lost or the loss is small. [15] Reduce the parameters by deleting the weights close to zero in the network. Pruning the filter can also effectively speed up the inference speed of the model. Compared with weight pruning, the advantage of filter pruning is that it does not cause network irregularities. There have been many methods for filter pruning, including weight norm [9], statistics of the next layer of information [16], scale of multiplier coefficient [17],etc. By pruning and retraining the network, these methods can reduce the network parameters while ensuring the accuracy of the model.

Quantization is also an effective way to compress the network. Quantization converts floating point operations to fixed point operations, that is, replacing high-precision numbers with low-precision numbers. Quantization can quantize the precision of all parameters in the network from 32 bits to 8 bits or lower [18]. In extreme cases, the weights in the network can even be quantified as binary [19-22] or ternary [23-24].

Knowledge distillation is to extract useful information from a complex network and migrate it to a smaller network to achieve the effect of network compression. Knowledge distillation was first proposed by Hinton [13] in 2015. The main idea is to distill the characteristics learned by the complex and strong learning ability network of teachers, and pass them to the student network with small parameters and weak learning ability. [25] proposed a method of FitNets, which trains student networks by combining intermediate-level hints in the hidden layer of the teacher. [26] By defining the attention of the network, the student network imitates the attention map of the teacher network, thereby improving the performance of the student network.

3. Method

SHEN et al [14] proposed a network similar to LeNet-5 called CS-CNN. It has a total of 6 layers, a custom convolutional layer after the input layer, uses SVD to compress the image, removes redundant information in the image, and then sends it to the convolutional network for convolution, which can effectively reduce the input layer parameters. At the same time, it can avoid overfitting.

Suppose matrix A is an $m \times n$ matrix, and the definition of SVD is:

$$A = U\Sigma V^T \tag{1}$$

Where U is an $m \times m$ matrix. Σ is an $m \times n$ matrix, which is all 0 except the elements on the main diagonal. Each element on the main diagonal is called a singular value. V is an $n \times n$ matrix. U and V are unitary matrices. If we multiply the transformation of A into A, we will get a square matrix A^TA. Then obtain its eigenvalues and eigenvectors by the following formula:

$$(A^TA)u_i = \lambda_i v_i \tag{2}$$

Then find the singular matrix Σ through the following process, where σ represents a singular value.

$$A = U\Sigma V^T \rightarrow AV = U\Sigma V^T V \rightarrow AV = U\Sigma \rightarrow Av_i = \sigma_i u_i \rightarrow \sigma_i = \frac{Av_i}{u_i} \tag{3}$$

In the singular value matrix, the singular values are arranged in descending order. The sum of the top 10% or even the top 1% of singular values accounts for more than 99% of the total singular value sum, which can compress the image and reduce the data the amount.

Quantization is to convert the floating-point operations of the neural network into fixed point operations. Since floating point operations in computers are more complex and less efficient than fixed-point operations. Neural networks are composed of floating-point operations, so convert floating-point operations into fixed-point operations. The calculation speed is greatly accelerated afterwards. The quantified formula is shown in the next.

$$x_{int} = round\left(\frac{x}{\Delta}\right) \tag{4}$$

$$x_Q = clamp(-(N_{levels}/2), N_{levels}/2 \quad 1, x_{int}) \quad if\ signed \tag{5}$$

$$x_Q = clamp(0, N_{levels} - 1, x_{int}) \quad if\ unsigned \tag{6}$$

Where Δ represents the quantized scaling factor, and x and x_{int} represent the numbers before and after quantization, respectively. When the quantization is 8 bits, $N_{levels=2^8}$, when the quantization is 4 bits, $N_{levels=2^4}$. By dividing by the scaling factor, the original floating point number can be converted into a cell.

The Figure.1 shows the framework description of the network.

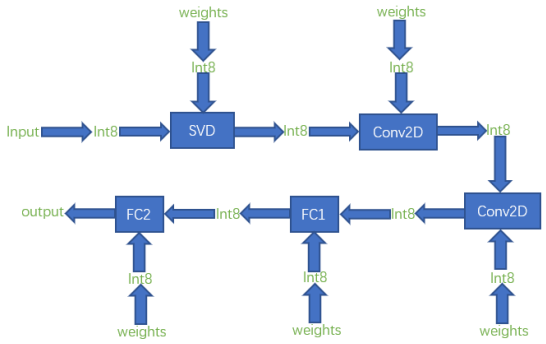


Fig.1 framework description

4. Experiments

In order to test the performance of the algorithm, this paper selects the MNIST handwritten digit recognition data set commonly used in image classification tasks as the experimental data set of this paper.

4.1. MNIST Handwritten Digit Dataset

MNIST is a handwritten digit recognition data set widely used in the performance test of image classification algorithms. It contains 70,000 handwritten digit image with a size of 28×28. Among them, 60,000 image are training data, and 10,000 image are test data. Each image in the MNIST data set represents a number from 0-9 and the number will

appear in the middle of the image.

4.2. Experimental Design

In order to verify the performance of the improved algorithm QCS-CNN in this paper, we use the MNIST handwritten digits data set to train the model. We evaluate the performance of the algorithm through the length of the training time of the model, the length of the test time and the accuracy.

4.3. Experimental Results

In Table 1, the time unit is seconds. We can see from the table that compared with the CS-CNN model, the training time and test time of the improved algorithm QCS-CNN are significantly reduced. This is because of the introduction of network quantification, which significantly reduces the amount of computations. The significant reduction in training time and test time shows that our improved algorithm performs better than the original algorithm. In the case of limited resources, we need to make an appropriate trade-off between resource consumption and algorithm accuracy. From Table 1, we can see that the accuracy of QCS-CNN is reduced by 0.48% compared to CS-CNN. This is due to the introduction of network quantization, which converts high-precision floating-point numbers into low-precision data, and some information will be lost. The training speed increased by 23.26%, and the test speed increased by 55.15%. At this time, the accuracy loss of 0.48% is within our acceptable range.

Table 1 result data

Model	Train Time	Test Time	Accuracy
CS-CNN	11.076	0.2796	98.41
QCS-CNN	8.5	0.1254	97.94

5. Conclusion

In this paper, we analyze and study the performance bottlenecks in deep neural networks and the current solutions. We propose an optimization algorithm QCS-CNN. On the basis of the CS-CNN algorithm, we introduced a method of network quantification. Quantization converts 32 bits floating point numbers into 8 bits int data, which reduces the amount of data computations and speeds up the model's inference speed. Through experiments, we proved the effectiveness of the QCS-CNN algorithm and achieved its goal of being applicable to resource-constrained devices.

References

[1] He K, Zhang X, Ren S , et al. Deep Residual Learning. for Image Recognition, 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2016.

[2] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E. Hinton.ImageNet classification. with deep convolutional neural networks. Commun. ACM 60, 6 (June2017),8490.DOI:https://doi.org/10.1145/3065386

[3] Ren, Shaoqing, et al. "Faster r-cnn:. Towards realtime object detection with region proposal networks." Advances in neural information processing systems. 2015.

[4] Joseph Redmon, Santosh Divvala, Ross Girshick, Ali Farhadi;You Only Look Once:. Unified, Real-Time Object Detection.Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 779-788

[5] Mariusz Bojarski,Davide Del Testa, Daniel Dworakowski,Bernhard Firner, Beat Flepp, Prasoon Goyal, Lawrence D Jackel, Mathew Monfort, Urs Muller, Jiakai Zhang, et al.End to end learning for self-driving cars. arXiv preprintarXiv:1604.07316, 2016.

[6] Simonyan, K., & Zisserman, A. Two-stream convolutional networks for action recognition in videos. In Advances in neural information processing systems pp. 568-576.2014.

[7] Kombrink, Stefan Mikolov, Tomáš Karafiát, Martin Burget, Lukáš (2011): "Recurrent neural network. based language modeling. in meeting recognition", In INTERSPEECH-2011, 2877-2880.

[8] G. Hinton et al., "Deep Neural Networks for Acoustic Modeling in Speech. Recognition: The Shared Views of Four Research Groups," in IEEE Signal Processing Magazine, vol. 29, no. 6, pp. 82-97, Nov. 2012, doi: 10.1109/MSP.2012.2205597.

[9] Li, H., Kadav, A., Durdanovic, I., Samet, H., and Graf, H. P., “Pruning Filters for Efficient ConvNets”, arXiv preprintarXiv:1608.08710, 2016.

[10] Han, S., Mao, H., and Dally, W. J., “Deep Compr.ession: Compressing Deep Neural Networks with Pruning, Trained Quantization and Huffman Coding”, arXiv preprintarXiv:1510.00149, 2015.

[11] Jaderberg, M., Vedaldi, A., and Zisserman, A., “Speeding up Convolutional. Neural Networks with Low Rank Expansions”,arXiv preprintarXiv: 1405.3866, 2014.

[12] Emily L. Denton, Wojciech Zaremba, Joan Bruna, Yann LeCun, Rob Fergus. Exploiting. linear structure

within convolutional networks for efficient evaluation. In NIPS, 2014. 1.
[13] Geoffrey Hinton, Oriol Vinyals, and Jeff Dean. Distilling the knowledge in a neural network. arXiv preprintarXiv:1503.02531, 2015.
[14] Y.Shen et al., "CS-CNN: Enabling Ro.bust and Efficient Convolutional Neural Networks Inference for Internet-of-Things Applications," in IEEE Access, vol. 6, pp. 13439-13448, 2018.
[15] Han S, Pool J, Tran J, et al. Learning both weights and connections for efficient neural network[C] Advances in neural information processing systems. 2015: 1135-1143.
[16] Jian-Hao Luo, Jianxin Wu, Weiyao Lin; ThiNet: A Filter Level Pruning Method for Deep Neural Network Compression.Proceedings of the IEEE International Conference on Computer Vision (ICCV), 2017, pp. 5058-5066.
[17] Zhuang Liu, Jianguo Li, Zhiqiang Shen, Gao Huang, Shoumeng Yan, Chang.shui Zhang;Learning Efficient Convolutional Networks Through Network. Slimming.Proceedings of the IEEE International Conference on Computer Vision (ICCV), 2017, pp. 2736-2744.
[18] Han, S., Mao, H., and Dally, W. J., "Deep Compression: Compressing Deep Neural Networks with Pruning, Trained Quantization and Huffman Coding", arXiv preprint arXiv:1510.00149, 2015.
[19] Courbariaux M, Bengio Y, David J P. Binaryconnect: Training deep neural networks. with binary weights during propagations[C] Advances in neural information processing systems. 2015: 3123-3131.
[20] Courbariaux, M., Hubara, I., Soudry, D., El-Yaniv, R., and Bengio, Y., "Binarized Neural Networks:. Training Deep Neural Networks with Weights and Activations Constrained. to +1 or -1", arXiv preprintarXiv:1602.02830, 2016.
[21] Mohammad Rastegari, Vicente Ordonez, Joseph Redmon, and Ali Farhadi. Xnor-net: Imagenet. classification using binary convolutional neural networks. In European Conference on Computer Vision, pages 525–542. Springer, 2016.
[22] Itay Hubara, Matthieu Courbariaux, Daniel Soudry, Ran El-Yaniv, and Yoshua Bengio. Quantized neural networks: training neural networks with low precision weights and activations. J. Mach. Learn. Res. 18, 1 (January 2017), 6869–6898.
[23] Zhu, C., Han, S., Mao, H., and Dally, W. J., "Trained Ternary Quantization". arXiv preprintarXiv: 1612.01064, 2016.
[24] Fengfu Li, Bo Zhang, and Bin Liu. Ternary weight networks.arXiv preprint arXiv:1605.04711, 2016.
[25] Romero, A., Ballas, N., Ebrahimi Kahou, S., Chassang, A., Gatta, C., and Bengio, Y., "FitNets: Hints for Thin Deep Nets", arXiv preprintarXiv:1412.6550, 2014.
[26] Zagoruyko, S. and Komodakis, N., "Paying More Attention to Attention:. Improving the Performance of Convolutional Neural Networks via Attention Transfer", arXiv preprintarXiv:1612.03928, 2016.

TROJAN TRAFFIC DETECTION BASED ON MACHINE LEARNING

MA ZHONGRUI[1], HUANG YUANYUAN[1], LU JIAZHONG[1*]

[1]School of Cybersecurity, Chengdu University of Information Technology, Chengdu, 610225, Sichuan, China
E-MAIL: 2020121052@stu.cuit.edu.cn, hy@cuit.edu.cn, *ljz@cuit.edu.cn

Abstract:

At present, most Trojan detection methods are based on the features of host and code. Such methods have certain limitations and lag. This paper analyzes the network behavior features and network traffic of several typical Trojans such as Zeus and Weasel, and proposes a Trojan traffic detection algorithm based on machine learning. First, model different machine learning algorithms and use Random Forest algorithm to extract features for Trojan behavior and communication features. Then identify and detect Trojans' traffic. The accuracy is as high as 95.1%. Comparing the detection of different machine learning algorithms, experiments show that our algorithm has higher accuracy, which is helpful and useful for identifying Trojan.

Keywords:

Trojan detection; Traffic analysis; Machine learning; Network behavior analysis

1. Introduction

Compared with other security threat programs, Trojan are more concealed and difficult to be detected by users in the background execution process. At the same time, this strong concealment feature also makes Trojan more harmful. Unlike other computer virus programs, it is different from many other virus programs that damage the important and private information of the user or the computer system, but collect and obtain the important information of the user, which unknowingly causes the privacy of the user damage. Under the attack of botnet Trojan, some computers will become so-called "bot host", and computer terminals can be used to carry out corresponding secondary attacks, causing greater security hazards.

With the emergence of many Trojan and the occurrence of Trojan attacks, researchers have attracted widespread attention to the problem of Trojan. The update and development of Internet technology is rapid, and the emergence and replacement of Trojan is also rapid. Today, the Internet is globally interconnected, and the major harm caused by Trojan attacks should arouse our close attention and research to help the healthy development of the Internet.

2. Related Work

H Thimbleby, Anderson S, Cairns P[1] analyzed the behavior features of Trojan based on the host, and gave a relatively formal definition of Trojan model. Christodorescu M, Jha S, Seshia SA, etc. [2] developed a malware detection model based on program semantics, trying to overcome the evasion technology of signature detection by encryption and deformation. Wang et al. [3] studied the characteristic paths of Trojan that are different from normal applications, and tried to detect Trojan by scanning the characteristic paths in the memory. Wu Xianda[4] used the monitoring and analysis of the entire traffic to detect the remote control Trojan program, and further processed the imbalanced data set through the Borderline-SMOTE algorithm. The entire process was exchanged between the Trojan control terminal and the controlled terminal. The asymmetry of the content is the feature to detect abnormal traffic. The Trojan detection method based on the attack tree model proposed by Yang Weijun and Zhang Shu[5] is to combine the features of the Trojan attack to establish the attack tree model of the related Trojan. However, the complexity of the entire algorithm makes the efficiency of traffic detection insufficient. Li Jianbin[6] proposed a method to establish a flow-based Trojan detection model to analyze the flow, classify and study massive amounts of flow data, and put forward corresponding solutions for P2P flow, Web flow, and conventional application flow. Recorded, and proposed a detection model based on knowledge base and behavior analysis. Wang et al.[7] used a detection method based on packet payload to detect data traffic, using deep packet inspection technology (Deep Payload In Spection, DPI) to detect Trojan communication traffic, and proposed that it can analyze the sensitive data in the communication load. The presence or absence of information can be used to detect network attacks and related malicious software. However, this method has a weaker ability to detect encrypted traffic and cannot better screen important information in a timely manner.

3. Our Methods

First, we need to capture Trojan traffic, distinguish the known Trojan traffic data packets from normal traffic data packets, and then match them in a certain proportion to form the final sample data set for machine learning algorithm model training. Part of the data extracted from the training data set is used as the test set to perform performance detection and evaluation on related algorithm models. The model will be trained by three different machine learning algorithms to ensure that the content of the training sample data set is basically the same for algorithm detection evaluation. As shown in Figure.1.

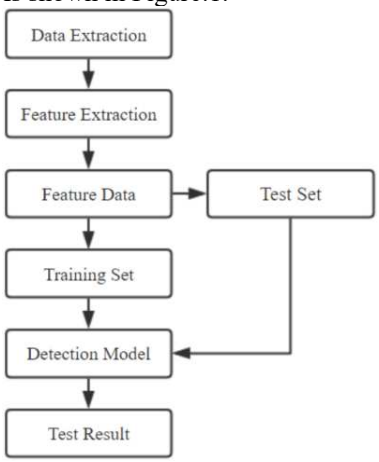


Fig.1 The basic flow of the detection method

The feature extraction work of CICFlowmeter is based on the original address and destination address of the flow data, that is, it can extract the relevant features during the conversation between hosts, including the size of the data flow and the session time of the communication between the hosts. , The size of the number of bytes of data packets transmitted by the two parties per second, etc., many of which are in line with the Trojan traffic features obtained after our analysis of the Trojan network behavior, so in order to obtain the features of the Trojan traffic data more accurately For the training set, we only need the feature information in the extracted feature files to filter, so as to wait for the training set of Trojan traffic features we finally need. As shown in Figure.2.

	A	B	C	D	E	F	G
1	Destinatio	Flow Dura	Total Fwd	Total Back	Total Leng	Total Leng	Fwd Packe
2	22	1266342	41	44	2664	6954	456
3	22	1319353	41	44	2664	6954	456
4	22	160	1	1	0	0	0
5	22	1303488	41	42	2728	6634	456
6	35396	77	1	2	0	0	0
7	22	244	1	1	0	0	0
8	22	1307239	41	40	2728	6634	456
9	60058	82	1	2	0	0	0
10	22	171	1	1	0	0	0
11	22	210	1	1	0	0	0
12	60060	75	1	2	0	0	0
13	35398	77	1	2	0	0	0
14	52320	2	2	0	2071	0	2065
15	52320	27701	15	6	18467	24	2920

Fig.2 Generated feature CSV file

This paper uses three different machine learning algorithms for model training and construction, namely Decision Tree, Naive Bayesian and Random Forest. The operation and use of related machine learning algorithms are realized by calling the API of the Weka platform. The single-room work of the model can be performed by calling the algorithm, and the algorithm can be adjusted and optimized to obtain different model training results.

4. Feature Extraction and Model Training

After obtaining the corresponding Trojan data traffic and normal application traffic, we need to extract the traffic features to obtain the feature training set for machine learning modeling. Here, the feature extraction method used in this article is to perform preliminary feature extraction through the open source feature extraction tool CICFlowmeter.

5. Experiment and Evaluation

5.1. Experimental Environment and Data

The experiment is conducted in a virtual machine intranet experiment environment built by a local computer and VMware, and the data set used is the IDS-2017 Trojan data set. Through the processing of the obtained data set, we selected three kinds of Trojan traffic data from various Trojan traffic data to conduct experiments, namely Weasel, Zeus and Zero Access Trojan traffic data. As shown in Table 1.

Table 1 Proportion of Trojan traffic in the data set

Zeus	26.4%
Zero Access	19.5%
Weasel	20.4%
Darkcomet	13.6%
Vantom	20.1%

5.2. Results and Evaluation

The model evaluation method of this experiment uses the percentage division method to evaluate the relevant machine learning algorithms, which ensures the fairness of the data to a certain extent. The training data set is divided into two parts. 70% is used for model training and 30% is used for detection.

The evaluation standard is the machine learning classification evaluation method [11], which detects and evaluates the three types of Trojan traffic respectively. The relevant introduction of this evaluation algorithm is as follows:

False Negative, FN. False Positive, FP. True Negative, TN. True Positive, TP.

Accuracy:

$$Accuracy = \frac{TP+TN}{TP+FN+FP+TN} \quad (1)$$

Precision:

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

The results of the experiment on Weasel:

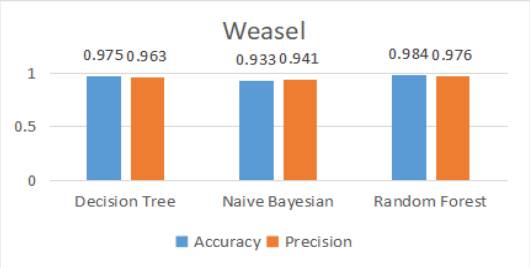


Fig.3 Model training Evaluation of Weasel Trojan

As can be seen from the data results in Figure.3, compared with the other two machine hash algorithms, the Random Forest has better detection performance for the Weasel Trojan traffic training model. The accuracy and precision are higher than the corresponding values of the other two machine learning algorithm models.

The results of the experiment on Zeus:

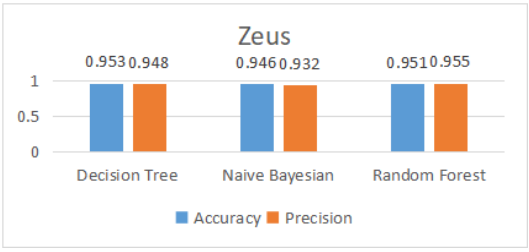


Fig.4 Model training Evaluation of Zeus Trojan

As can be seen from the above figure, the evaluation results of the models trained by each algorithm are relatively similar, but by comparison, the difference between the accuracy and precision of the Decision Tree algorithm and the Random Forest algorithm model is relatively small. and the accuracy is more than 95%.

The results of the experiment on Zero Access:

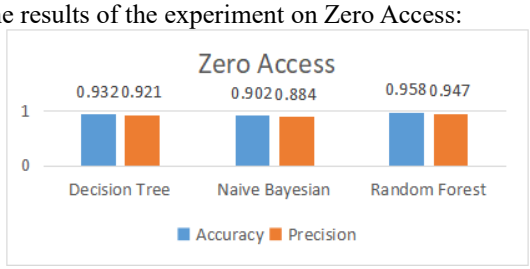


Fig.5 Model training Evaluation of Zero Access Trojan

Through the observation of the accuracy data in the above table, we can see that only the Random Forest algorithm reaches more than 95% and the precision is about 95%, while the precision of the Naive Bayesian algorithm is only less than 90%, and its accuracy is only about 90%.

In addition, this paper also uses F1 score (F1-Score) and recall rate to evaluate different machine learning algorithm models. F1 score is usually used to measure the accuracy of two-classification or multi-task two-classification model, taking into account the accuracy and recall rate of the classification model.

The formula for scoring F1 is as follows:

$$F1 = \left(\frac{recall^{-1}+precision^{-1}}{2}\right)^{-1} = 2 * \frac{precision*recall}{precision+recall} \quad (3)$$

The recall rate formula is as follows:

$$r = \frac{TP}{TP+FN} \quad (4)$$

Weasel:

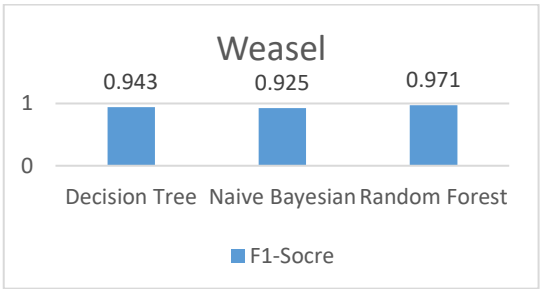


Fig.6 Model score for Weasel

Zeus:

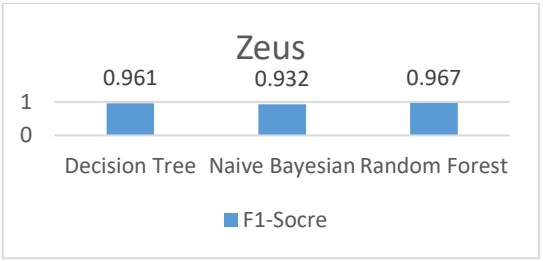


Fig.7 Model score for Zeus

Zero Access:

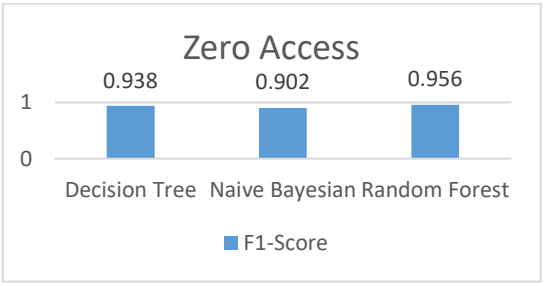


Fig.8 Model score for Zero Access

6. Conclusions

By comparing the various data in the above statistical graphs, we can see that the performance of the three different models established by the Naive Bayesian algorithm for the three types of Trojan traffic is relatively lower than that of the other two machine learning algorithms. In terms of the fluctuation of values, the fluctuation of the relevant values of each model of the Decision Tree algorithm is relatively small, and the performance is relatively stable. However, from all aspects, the evaluation accuracy and precision of the model trained by the Random Forest algorithm are higher than the other two machine learning algorithms, and it can also be seen from the evaluation of each model performed by the F1-Score value that the Random Forest algorithm Compared with the other two machine learning algorithms, the Random Forest algorithm has a better model detection effect. Compared with the other two machine learning algorithms, the model of the Random Forest algorithm is composed of a large number of base learners. The cooperation of different base learners makes the algorithm have better classification capabilities. It can be understood that the model based on the Random Forest algorithm has better performance for Trojan traffic detection than the other two machine learning algorithms, and is more suitable for the detection of Trojan traffic data.

References

[1] Thimbleby H, Anderson S, Cairns P. A Framework for Modelling Trojans and Computer Virus Infection[M]. Computer Journal, 1998, 41(7): 444-458,1998

[2] Christodorescu M, Jha S, Seshia S A, et al. Semantics-aware malware detection[M]. In: Security and Privacy, Oakland:IEEE, 2005. 32-46,2005

[3] Wang, R., Wang, W., Gong, X., Que, X., & Ma, J. (2010, April). A Real-Time Video Stream Key FrameIdentification Algorithm for QoS[M]. In Multimedia and Information Technology (MMIT), 2010 Second International Conference on (Vol. 1, pp. 115-118). IEEE, 2010

[4] Wu Xianda. Remote control Trojan detection model based on abnormal network behavior [D]. Beijing University of Technology, 2018

[5] Yang Weijun, Zhang Shu, Hu Guangjun. Trojan detection method based on attack tree model[J]. Information Network Security, 2011(09): 170-172

[6] Li Jianbin. Trojan detection technology based on traffic [D]. University of Electronic Science and Technology of China, 2014

[7] Wang Zhanhao. Research on Trojan Attack and Prevention Technology [J]. Shanghai Jiaotong University, 2007

EARLY DETECTION OF COVID-19 DISEASE USING COMPUTED TOMOGRAPHY IMAGES AND OPTIMIZED CNN-LSTM

MUHAMMAD HAMMAD MEMON[1,2], NOORBAKHSH AMIRI GOLILARZ[2], JIANPING LI[2], MOHAMMAD YAZDI[3], ABDOLJALIL ADDEH[4]

[1]Faculty of Artificial Intelligence and Big Data, Yibin University, Yibin, 644000, China
[2]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[3]Instituto Superior Técnico, University of Lisbon, 1049-001 Lisbon, Portugal
[4]Faculty of Electrical and Computer Engineering, Babol Noshirvani University of Technology, Babol, Iran
E-MAIL: muhammadhammadmemon@yahoo.com, noorbakhsh.amiri@std.uestc.edu.cn, jpli2222@uestc.edu.cn, mohammad_yazdi@live.com, jalil_addeh@yahoo.com

Abstract:

Since the novel Coronavirus (COVID-19) pandemic showed up in China, it became a big problem for health authorities to counter this life-threatening disease. Early light signs such as fever and nonproductive cough give a chance for early detection of disease and appropriate treatment. Imaging features that can be obtained using computed tomography (CT) images are of the most significant aspects of COVID-19 for screening, examination, therapy evaluation, and follow-up. This paper proposes an intelligent method for early detection of COVID-19 based on CT images and deep neural networks. In the developed method, the convolutional neural network (CNN) is used for automatic feature extraction from CT images and long-short term memory (LSTM) is used for final classification. Moreover, the Harris hawk optimization (HHO) algorithm is implemented for finding the best possible value of internal parameters of CNN and LSTM, such as the number of convolution/pooling layers, size, and the number of convolution kernels with the aim of increasing the classification accuracy. The developed method tested on data collected in Mashi Daneshvari Hospital in Iran. The obtained results showed that the developed method could detect the COVID-19 with high accuracy without needing radiologist experts.

Keywords:

CNN; LSTM; Biomedical image processing; Machine-learning algorithms; Optimization

1. Introduction

Coronavirus disease 2019 (COVID-19) was firstly identified in Wuhan city, China, in December 2019, and has since been distributed around the world, which leads to a continuing pandemic. As of 24 October 2020, more than 42.4 million cases have been identified throughout 187 different countries and territories, resulting in more than 1.15 M deaths. [1]. Due to COVID-19 's strong and growing infectivity, fast and effective diagnostic methods are immediately aimed to determine, isolate, and treat patients as quickly as possible [2].

The signs of this infective respiratory disease are nonspecific, ranging from asymptomatic to severe pneumonia and death. Low-grade or high-grade fever and nonproductive cough are the most frequent medical symptoms [3]. In order to validate the diagnosis of COVID-19, a particular viral nucleic acid assay using real-time transcription-polymerase chain reaction (RT-PCR) was grown rapidly. However, some patients with a probable COVID-19 infection might just have initial negative RT-PCR results from the recently published research literature. The major reason for falsified-negative RT-PCR testing generally involves insufficient cellular material for detection and improper nucleic acid removal from clinical materials [4]. In accordance with obtained experiences through the past four months, chest computed tomography (CT) imaging may manifest abnormalities in advance of the RT-PCR approach. Currently, high-resolution chest computed tomography imaging has been included as one of the main tools for screening, primary diagnosis, and evaluation of disease severity [4].

Particularly in comparison to RT-PCR, a chest computed tomography scan may be a much more reliable, effective, and rapid technique for the classification and evaluation of COVID-19, especially in the epidemic region [5]. Nearly all hospitals have CT imaging machines; thus, the computed tomography images of the chest can be used to classify and identify COVID-19 patients in advance. The existence of infected air sacs (called alveoli) inside the lungs is usually reflected in the computed tomography images.

However, using computed tomography images for COVID-19 detection is not a perfect approach. Radiologists still find it challenging to distinguish between infected and uninfected lungs. Unfortunately, with a visual inspection, this suffers from the unavoidable human mistake and malfunction, which can be further amplified by the low quality of computed tomography images. Many researchers believe that automating computed tomography screening analyzes tends to increase the early detection rate [6].

In the recent time, thresholding [7-8], neural network [9-10], and several deep learning algorithms, especially convolutional neural networks (CNN) and long-term memory (LSTM), have been proposed for solving numerous complex tasks in all forms of image de-noising (preprocessing) and analysis, e.g., neuro, retinal, digital anatomy, abdominal, musculoskeletal pulmonary, breast, neurological, and the other medical image processing [11]. In recent years, end-to-end trained CNNs have now become the preferred approach for interpreting medical imaging [12]. If the input image is not noise-free, CNNs may derive useful and important information from it because of its noise-insensitivity. These output characteristics are expressed in a network structure that is layer by layer. As the layers in the network deepen, features are learned and represented more abstractly and concisely.

Aside from CNN, LSTM is another form of deep learning algorithm commonly used for time series analysis. It has been utilized in other applications, such as natural language processing, voice synthesis, and synthesis of handwriting [13]. The connections between the LSTM units allow information to cycle over the adjacent time-steps through a loop. This provides an internal feedback environment, which helps the network to understand the meaning of time and to learn about the temporal structure within the data presented.

Considering the importance of early and accurate detection of COVID-19, a simple, fast and accurate method is proposed in this study. The proposed method does not require the extraction of new features manually from chest CT images or human-based interpretation. In the proposed method, ConvNet is used for the extraction of new features from chest CT images, and LSTM is used for classification. Moreover, Harris hawk optimization (HHO) algorithm is used to find an optimal value of internal parameters of the CNN and LSTM, such as a number of convolution/pooling layers, size, and the number of the filter with the aim of increasing the classification accuracy and reducing the computational complexity. The HHO algorithm is one of the most accurate and fast nature-based optimization algorithms that mimic Harris hawk's behavior in nature [14] and it has been applied in various problems [15-19]. In recent years, nature-based optimization algorithms have been successfully used in many engineering tasks [20-24] [26-32].

2. Proposed Method

Given the important role of chest computerized tomography images in COVID-19 detection in early stages, it is significantly essential for physicians and practitioners to become acquainted with the regular features of computerized tomography images resulting from COVID-19. Despite the fact that regular and irregular computerized tomography images findings of COVID-19 are announced in the literature, the computerized tomography image features of COVID-19 overlies with those of viral pneumonia and other breathing illnesses. Consequently, it is an extremely difficult task for radiologists to make an exclusive and accurate diagnosis. Moreover, it is found that the COVID-19-infected patients show some pattern on chest computerized tomography images, which is not easily detectable by the human eye. Therefore, it is significantly important to develop an automatic method for computerized tomography images analysis for accurate detection of COVID-19. This paper proposes an intelligent method based on CNN and LSTM for chest CT image analysis and COVID-19 detection. The proposed method includes three main modules: a feature extract module, a classification module, and an optimization module.

In the case of any pattern recognition problem, extracting as much information as possible from the available data sets is crucial to creating an effective solution. Most of the time, researchers extract new features from raw data based on their experience that is called handcrafted feature engineering. This type of feature engineering has some drawbacks. First, manual feature engineering can be a tedious process. Secondly, it is boring. Moreover, the influence of human bias can lead the feature extraction process to the wrong route. These problems can be solved using CNNs. Numerous convolutional and pooling layers in the CNN structure shape a deep and rich network for extracting the fundamental characteristics form the input image.

In the feature extraction of the proposed method, we used CNNs for generating effective and abstract features from computerized tomography images that cannot be seen or detected by a human expert. The automatically extracted features lead to more accurate infection detection and classification. The LSTM network has the ability to learn chronological correlations and long-term dependencies. The LSTM network and CNN could complement each other by learning long-term dependency and local trends independently. Therefore, in the classification module of the proposed method, we used LSTM for the final classification.

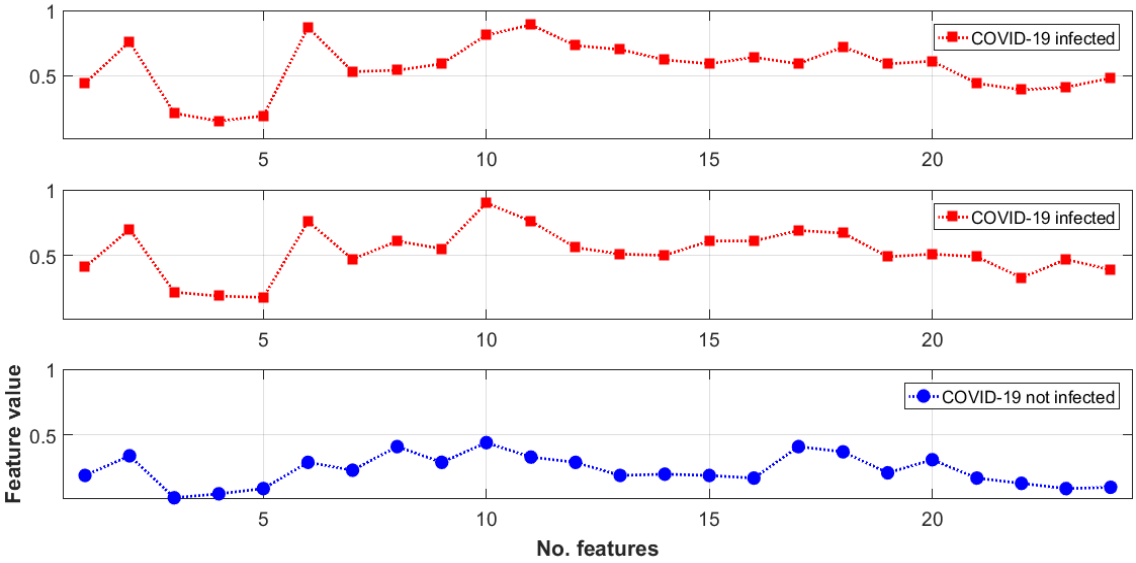


Fig.1 Extracted features from CT images by CNN

One great obstacle for implementing CNN and LSTM networks on a new problem is that it requires the amount of considerable experience and skill to select fitting hyper-parameters such as activation function type in CNN, number of convolution, and pooling layer in CNN and number of memory blocks in LSTM network. Since these hyper-parameters have internal relations, their tuning is notably expensive and time-consuming. These hyper-parameters are the number of layers, learning rate, activation function type, number and size of kernels zero-S, P, pooling method type, size of kernels in pooling layer, stride, and the number of memory blocks in LSTM. This paper proposes the application of the HHO algorithm for finding the optimal value of hyper-parameters in CNN and the LSTM network.

3. Results

3.1. Dataset

In this study, the chest CT images dataset collected in the National Research Institute of Tuberculosis and Lung Diseases (NRITLD), Daneshvari Hospital, Tehran, Iran, is used for evaluation of the developed method [25]. The dataset is collected by three experienced radiologists with 15, 10, and 17 years of clinical experience between March 2020 and May 2020. From the 315 cases, 174 cases are patients confirmed with COVID-19, and 141 cases are patients with other respiratory diseases such as Pneumonia, Emphysema, and Asthma that are confirmed by an experienced radiologist. Table 1 lists the details of a dataset.

Table 1 Details of dataset

Class	Gender	No. cases	Age range
COVID-19	Male	93	[18 73]
	Female	81	[23 79]
Other respiratory diseases	Male	73	[19 75]
	Female	68	[20 74]

We used K-folds cross-validation with K=4 to split our data into training and test subsets. All the simulations are performed using a personal computer with core i7 processing cores and 16 GB RAM and Python programming language.

3.2. Performance of the proposed method

In this subsection, the performance of the proposed method is evaluated. For this purpose, hyper-parameters are selected using the optimization algorithm. In the HHO algorithm, 30 hawks are generated randomly in the search space, and the optimization process is iterated 100 times. The selected hyper-parameters using HHO algorithm are listed in Table 2. According to the HHO algorithm, CNN with five layers (NL=5) and learning rate equal to 0.0018 and LSTM network with 43 memory blocks (NMB=43) leads to the highest accuracy.

Figure.1 shows the extracted features by convolution layers with optimal structures. It can be seen that the input CT images are converted to a vector with 24 arrays. Each array in the feature vector indicates the deep feature of CT image. Using CNN, 24 effective features were extracted and used as the input of LSTM. The simulations showed that the proposed

method, CNN-LSTM optimized by the HHO algorithm, could classify the COVID-19 with 99.37% accuracy.

Table 2 Optimal configuration

	T_{Act}	NK_c	SK_c	S_c	Z	$T_{pooling}$	SK_p	S_p
Raw data	–	–	–	–	–	–	–	–
Layer 1	RReLU	64	5×5	1	1	L_p	4×4	1
Layer 2	PReLU	128	4×4	2	1	L_p	3×3	1
Layer 3	PReLU	256	4×4	1	2	Mixed	3×3	2
Layer 4	PReLU	32	3×3	2	2	L_p	2×2	1
Layer 5	RReLU	32	3×3	1	1	L_p	2×2	1

4. Conclusion

The number of cases of COVID-19 continues to rise in Iran and around the world. In this condition, timely diagnosis of the disease in the early stages can help physicians to adopt the right decisions and choose appropriate remedies methods, and ultimately increase the chances of survival of the patient to a very high level. According to the importance of the issue, in this study, a new hybrid method was presented to process a CT scan of chest images and diagnosis of COVID-19 disease. In this method, CNN was used for the automatic extraction of characteristics and the LSTM network for the final classification of images. Also, the HHO algorithm was used to select the optimal parameters of CNN and the LSTM neural network. The proposed method can diagnose the disease with an accuracy of 99.37%. The results showed the superiority of the proposed method over other techniques available in the literature.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, the project of Science and Technology Department of Chongqing Municipality, Chengdu Chengdian Network Technology Co., Ltd., Chengdu Civil-military Integration Project Management Co., Ltd., and Sichuan Yin Ten Gu Technology Co., Ltd.

References

[1] World Health Organization. https://www.who.int. [Accessed May 2020]

[2] K. Imai, S. Tabata, M. Ikeda, S. Noguchi, and T. Maeda, "Clinical evaluation of an immunochromatographic IgM/IgG antibody assay and chest computed tomography for the diagnosis of COVID-19," Journal of Clinical Virology, vol. 128, Article 104393, 2020.

[3] M. Vaduganathan, O. Vardeny, T. Michel, J.J.V. McMurray, M.A. Pfeffer, and S.D. Solomon, "Renin-Angiotensin-Aldosterone system inhibitors in patients with Covid-19," The New England Journal of Medicine, vol. 382, pp. 1653-1659, 2020.

[4] C. Long, H. Xu, Q. Shen, X. Zhang, B. Fan, C. Wang, B. Zeng, Z. Li, X. Li, and H. Li, "Diagnosis of the Coronavirus disease (COVID-19): rRT-PCR or CT?," European Journal of Radiology, vol. 126, Article 108961, 2020.

[5] N. Chen, M. Zhou, and X. Dong, "Epidemiological and clinical characteristics of 99 cases of 2019 novel coronavirus pneumonia in Wuhan, China: a descriptive study," Lancet, vol. 395, pp. 507-513, 2020.

[6] H. Liu, F. Liu, J. Lia, T. Zhang, D. Wang, and W. Lan, "Clinical and CT imaging features of the COVID-19 pneumonia: Focus on pregnant women and children," Journal of Infection, vol. 80, no. 5, pp. 7-13, 2020.

[7] N. A. Golilarz, N. Robert, J. Addeh and A. Salehpour, "Translation Invariant Wavelet based Noise Reduction using a New Smooth Non-linear Improved Thresholding Function," CRPASE, Vol. 3, No. 3, pp. 104–108,2017.

[8] N. A. Golilarz and H. Demirel, "Image De-noising using Un-decimated Wavelet Transform (UWT) with Soft Thresholding Technique," Proceeding of IEEE CICN2017 Conference, pp. 16-19, September 2017.

[9] N. A. Golilarz and H. Demirel, "Thresholding Neural Network (TNN) with Smooth Sigmoid based Shrinkage (SSBS) Function for Image De-noising," Proceeding of IEEE CICN2017 Conference, pp. 67-71, September 2017.

[10] N. A. Golilarz and H. Demirel," Thresholding Neural Network (TNN) based Noise Reduction with a New Improved Thresholding Function," CRPASE, Vol. 3, No. 2, pp. 81–84, 2017.

[11] Izadpanahkakhk, M.; Razavi, S.M.; Taghipour-Gorjikolaie, M.; Zahiri, S.H.; Uncini, A. Deep Region of Interest and Feature Extraction Models for Palm print Verification Using Convolutional Neural Networks Transfer Learning. Appl. Sci. 2018, 8, 1210.

[12] Abbasian Ardakani, A.; Rajabzadeh Kanafi, A.; Acharya, U.R.; Khadem, N.; Mohammadi A. Application of deep learning technique to manage COVID-19 in routine clinical practice using CT images: Results of 10 convolutional neural networks.

Computers in Biology and Medicine 2020, 121, Article 103795.

[13] N. Lv, X. Liang, C. Chen, Y. Zhou, J.Li, H. Wei, and H. Wang, “A long Short-Term memory cyclic model with mutual information for hydrology forecasting: A Case study in the xixian basin,” Advances in Water Resources, vol. 141, Article 103622, 2020.

[14] A. A. Heidari, S. Mirjalili, H. Faris, I. Aljarah, M. Mafarja, and H. Chen, “Harris hawks optimization: Algorithm and applications,’" Future Generation Computer Systems, vol. 97, no. 3, pp. 849-872, 2019.

[15] N. Amiri Golilarz, A. Addeh, H. Gao, L. Ali, A. Moradkhani Roshandeh, H. Mudassir Munir, and R. U. Khan, “A New Automatic Method for Control Chart Patterns Recognition Based on ConvNet and Harris Hawks Meta Heuristic Optimization Algorithm,” IEEE Access, vol. 7, pp. 149398- 149405, 2019.

[16] N. Amiri Golilarz, H. Gao, R. Kumar, L. Ali, Y. Fu, C. Li, “Adaptive Wavelet Based MRI Brain Image De-noising,” Frontiers in Neuroscience, Vol. 14:728, 2020.

[17] N. Amiri Golilarz, H. Gao, and H. Demirel, “Satellite image De-noising with harris hawks meta heuristic optimization algorithm and improved adaptive generalized Gaussian distribution threshold function,” IEEE Access, Vol. 7, pp. 57459–57468, 2019.

[18] N. A. Golilarz *et al.*, “Optimized wavelet-based satellite image de-noising with multi-population differential evolution-assisted harris hawks optimization algorithm,” *IEEE Access,* vol. 8, pp. 133076-133085, 2020.

[19] M. Shahid, J. P. Li, N. Amiri Golilarz, A. Addeh, J. Khan, and A. Ul Haq, “Wavelet Based Image DE-Noising with Optimized Thresholding Using HHO Algorithm,” 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, Chengdu, China, 2019.

[20] J. Addeh, and A. Ebrahimzadeh, “Breast Cancer Recognition Using a Novel Hybrid Intelligent Method,” Journal of Medical Signals and Sensors, vol. 2, pp. 22-30, 2012.

[21] Abdoljalil Addeh, Aminollah Khormali, Noorbakhsh Amiri Golilarz. Control chart pattern recognition using RBF neural network with new training algorithm and practical features. ISA Transactions, 79 (2018) 202-216.

[22] A. Khormali, and J. Addeh, “A novel approach for recognition of control chart patterns: Type-2 fuzzy clustering optimized support vector machine,” ISA Transactions, vol. 63, pp. 256-264, 2016.

[23] Memon, Muhammad Hammad , et al. "Breast Cancer Detection in the IOT Health Environment Using Modified Recursive Feature Selection." Wireless Communications and Mobile Computing (2019).

[24] Memon, Muhammad Hammad , et al. "Early Stage Alzheimer's Disease Diagnosis Method." 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP) 2020.

[25] The National Research Institute of Tuberculosis and Lung Diseases(NRITLD), Daneshvari Hospital, http://www.en.nritld.sbmu.ac.ir, [Accessed in 1 June 2020]

[26] J. Addeh, A. Ebrahimzadeh, and V. Ranaee. “Application of the PSO-RBFNN Model for Recognition of Control Chart Patterns”. 2nd International Conference on Control, Instrumentation and Automation (ICCIA), Shiraz, Iran, 2011 (IEEE, Citation: 9)

[27] Alireza Khosravi, Ali Lari, Jalil Addeh. “A New Hybrid of Evolutionary and Conventional Optimization Algorithms”. Applied Mathematical Sciences, 6 (2012) 815 – 825.

[28] A. Khosravi, J. Addeh, and J. Ganjipour. “Breast Cancer Detection Using BA-BP Based Neural Networks and Efficient Features”. 7th Iranian IEEE Conferences on Machine Vision and Image Processing (MVIP), Tehran, Iran, 2011.

[29] Payam Zarbakhsh, Abdoljalil Addeh. “Breast cancer tumor type recognition using graph feature selection technique and radial basis function neural network with optimal structure”. Journal of Cancer Research and Therapeutics, 14 (2018) 625-633

[30] Ataollah Ebrahimzadeh, Jalil Addeh, Zahra Rahmani. “Control Chart Pattern Recognition Using K-MICA Clustering and Neural Networks”. ISA Transactions, 51 (2012) 111–119.

[31] J. Addeh, A. Ebrahimzadeh, and V. Ranaee. “Control Chart Pattern Recognition Using Adaptive Back-propagation Artificial Neural Networks and Efficient Features”. 2nd International Conference on Control, Instrumentation and Automation (ICCIA), Shiraz, Iran, 2011 (IEEE, Citation: 11)

[32] L. Ali, C. Zhu, Z. Zhang, Y. Liu, “Automated Detection of Parkinson’s Disease Based on Multiple Types of Sustained Phonations Using Linear Discriminant Analysis and Genetically Optimized Neural Network”. IEEE Journal of Translational Engineering in Health and Medicine, vol. 7, 2019.

EASY DATA AUGMENTATION METHOD FOR CLASSIFICATION TASKS

LIU GUOHANG[1], ZHANG SHIBIN[1], TANG HAOZHE[1], YANG LU[1], LU JIAZHONG[1], HUANG YUANYUAN[1]

[1]School of Cybersecurity, Chengdu University of Information Technology, Chengdu 610225, China
E-MAIL: a_wall@aliyun.com, cuitzsb@cuit.edu.cn

Abstract:

In recent years, the rapid development of deep learning has made great progress in artificial intelligence-related technologies. With the deepening of artificial intelligence research, machine learning is applied to more and more fields. Although machine learning has many advantages and has achieved considerable results, machine learning and its related learning algorithms still face some related challenges. That is, the lack of sufficient training data or uneven class balance in the data set. In deep artificial neural networks, a large amount of training data is needed to learn effectively, and collecting such training data is often expensive and laborious. Data Augmentation overcomes this problem by artificially expanding the training set and label retention conversion. In this article, we propose a method to expand the data set based on ball k-means. The experiments on the Four-class, Digits, Iris and Breast-cancer data sets prove the efficiency of the method--fast execution speed, low computational complexity, and the effectiveness of the method. In these experiments, the quality of the training model has been improved, but the learning time stays the same as when the enhancement method is unused.

Keywords:

Data augmentation; Machine learning; Deep learning; K-means

1. Introduction

With the continuous development of artificial intelligence technology, more and more industries can use machine learning methods to make breakthroughs. However, the lack of a large number of available data sets has become a bottleneck in the progress of artificial intelligence. Traditional data augmentation methods are mainly used in the field of image classification, and there are a series of problems such as manual extraction, cumbersome and difficult feature processing, and low efficiency. Data augmentation is an important part of the training process applied to machine learning models. The reason is that the training process for machine learning models, especially deep learning, relies on large labeled data sets, which are expensive to acquire, store, and process. Therefore, a reasonable alternative is to be able to use a process called data augmentation to automatically generate new labeled training samples. The main method of Data augmentation in this field is to assume that new training samples can be obtained through random geometry or appearance transformation applied to the tagged training samples, but this is a strong assumption as it is not clear for whether this is a reliable generation model for generating new training samples. Therefore, how to effectively expand data has become one of the hot research directions in the field of artificial intelligence. At present, researchers have conducted a lot of studies on data augmentation. The existing data augmentation methods mainly include:

Chatfield et al. [1] explored the differences between them by evaluating different CNN architectures on a common data set. His research mainly focuses on the rigorous evaluation of deep structure and shallow coding methods, also, it includes the evaluation of three enhancement methods. Mash et al. [2] used a fine-grained data set containing 10 classes to classify various geometric enhancement methods for aircraft classification tasks. The extended methods tested the objects include cropping, rotation, rescaling, polygon occlusion, and combinations of these methods. Luke Taylor et al. [4] used a relatively simple CNN based on the use of CNN by Zeiler and Fergus [3] to evaluate various popular geometric and photometric enhancement schemes on the coarse-grained Caltech101 data set, with the goal of contributing to deep learning Empirical data in the field so that researchers can choose the most suitable general amplification scheme for the data set for the given conditions.

On the whole, the current research methods for expanding data sets are mainly aimed at the field of image classification, but there is a lack of research on traditional classification tasks. How to select features reasonably, process feature values properly, and expand effectively is still a difficult problem to face. At the same time, there is currently no universal expansion scheme for different data sets. Therefore, in view of the limitations of the current mainstream data augmentation methods, this paper proposes a general data augmentation method that does not rely on feature value extraction and preprocessing based on the

unsupervised learning method. The method in this paper combines ball k-means cluster [5], normal distribution model and purity theory to expand data simply and efficiently.

The main contributions of this paper are as follows: (1) Introduce the granular ball theory in the ball k-means and the normal distribution in statistics, and then perform unsupervised learning clustering on the original data set, and divide the stable area. A large number of new data conforming to the normal distribution is generated in the stable area of the ball cluster, which greatly reduces the clustering time and ensures that the expanded data is highly correlated with the center of the ball cluster. （2) Introduce the purity to perform simple and effective automatic labeling of clustered ball cluster data to further accelerate it. (3) Multiple comparative experiments show that the method proposed in this paper can make the classifier have higher accuracy and precision.

2. Data augmentation method

The general architecture of the data augmentation method proposed in this paper is shown in Figure 1. We first divide the data set into training set and test set according to the proportion of 7:3, and then input the training set into the ball k-means cluster. After the clustering results are obtained, the data in the sphere cluster expanded, then the expanded data is marked according to the purity theory, and a large number of data with obvious characteristics and marked data are obtained. After that, it needs to be input into the training module to obtain the classifier model. Finally, the test set is input into the classifier model for verification and output the results. Next, the proposed method will be introduced in detail according to the modules.

2.1. Ball k-means

In this paper, the ball k-means algorithm and granular ball theory are introduced to cluster the training set. This cluster uses hyper spheres to divide the metric space clusters, in order to obtain neighbor relationships more accurately without additional parameters, to eliminate a single sample The upper and lower bounds that need to be maintained greatly to improve the efficiency of the k -means algorithm.The ball k-means algorithm divides ball clusters and neighboring ball clusters to obtain the stable areas of each ball cluster. The relationship between ball cluster and the stable area is shown in Figure 2. Each blue circle represents a ball cluster, and each red circle represents the stable area of the corresponding ball cluster.

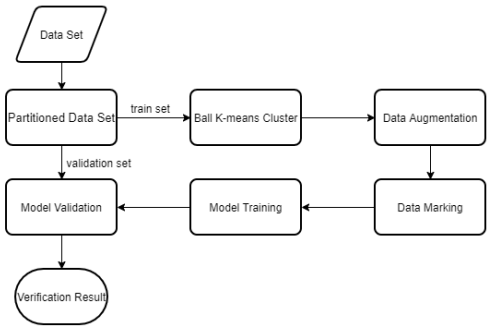


Fig.1 Overall frame design

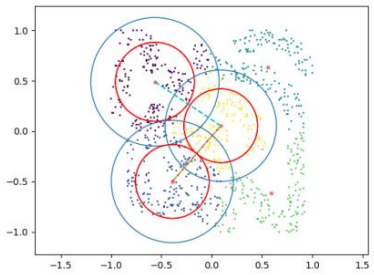


Fig.2 Ball clusters and stable areas

In the ball k-means cluster, we only need to enter the number of clusters called n. Then we can quickly and efficiently obtain the divided ball clusters and the corresponding stable domains. We initialize n equal to the number of categories of the data set, and continuously adjust the value of n according to the model verification results to receive the best effect. Since the hyper sphere model only uses the radius and center to describe a cluster, a more accurate description of the spatial relationship is obtained, which is simple but efficient, and the speed is greatly improved. The following describes in detail about the process of using the ball k-means cluster to obtain ball clusters and the stable areas. Here come the steps:

(1) Input the training set, and initialize the center randomly, and then set the initial cluster number n as the number of categories of the data set. Output the final ball cluster center c, which is the mean value of all points in the ball cluster。

(2) According to the multi-granularity-particle sphere calculation theory, the radius $r = \max(||x_i - c||)$ of the sphere cluster is calculated, and r represents the distance from the farthest point in the sphere cluster to the center (c) of the sphere cluster, and x_i represents any single point in the sphere cluster.

(3) Calculate the distance between the centers of each sphere cluster, and get the neighbor sphere cluster $\{N_{C_i}\}$ of

each sphere cluster. The definition of the neighbor sphere cluster is as follows:

Given two ball clusters C_i and C_j, the corresponding centers are c_i and c_j. If the radius r_i of C_i is satisfies the condition $\frac{1}{2}||c_i - c_j|| < r_i$, we insist C_j is the neighbor ball cluster of C_i.

(4) By searching the neighboring ball clusters of each ball cluster, the stable area is obtained. The definition of stable area is as follows:

If $C_j \in \{N_{C_i}\}$, then the stable area of C_i is centered on the center of the ball clusterC_i, and $\frac{1}{2}\min(||c_i - c_j||), c_j \in N_{c_i}$ is used to calculate the radius.

2.2. Data augmentation

In the ball k-means cluster, the points in the stable domain do not need to be adjusted during the next iteration. We can think that the points in the stable area are highly correlated with the center of the ball cluster. At the same time, we introduce the normal distribution in statistics to generate a large number of points conforming to the normal distribution in the stable area to achieve the effect of data augmentation. These expanded points have the characteristics of normal distributions, and a strong correlation with the center of the ball cluster, which can effectively represent the real data. The amount of data we initially set to expand is consistent with the original data set. The expanded data in the ball cluster is shown in Figure 3. The blue dots represent the data expanded by the normal distribution model.

2.3. Data marking

After using the ball k-means to cluster the training set and utilizing the normal distribution to expand data, the expanded data needs to be labeled. This article introduces the purity which is used for marking the extended data. Purity is a simple and transparent evaluation method, and it is convenient for calculation. This method improves the effect of the model in this paper greatly. The following describes the process of using the purity algorithm to label data in detail.

(1) For a cluster, we first calculate P_{ij}, P_{ij} refers to the probability that whether a point in cluster i belongs to class j.

(2) We input clustering results and the expanded data of ball k-means cluster, and then calculate the purity of each ball cluster through clustering results. What is more, we mark the points in the corresponding ball clusters according to the purity.

The label of each ball cluster is marked on the expanded data. Finally, output the labeled extended data and mix it with the original training set to obtain a new one. At this point, the data augmentation work has completed, and then the new training set can be input into the classifier for training.

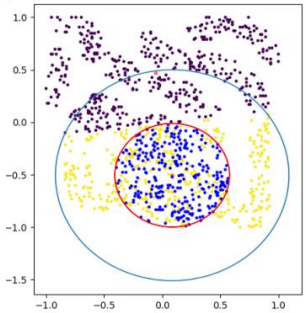


Fig.3 Use the normal distribution model to expand the data

2.4. Classification module

This article chooses to use SVM classifier, Naive Bayes classifier and random forest classifier to train the model separately respectively. These three classifiers are the most commonly used classifiers in machine learning, and the trained model is very representative.

3. Experimental analysis

3.1. Experimental setup

This article selects the following criteria to evaluate the proposed methods: accuracy, recall and precision. The experimental results are expressed by the expanded index minus the original data index and they are named: AD (Accuracy Difference), RD (Recall Difference), and PD (Precision Difference). Namely: AD=new accuracy-old accuracy.

3.2. Data sets

This article uses a number of classic data sets for experiments, namely: Four-Class data set, Digits data set, Iris data set and Breast-cancer data set.

3.3. Experimental data

3.3.1. Comparative experiment

In the comparative experiment part, we used the four classifier models in section 2.4 to test the original and extended data sets.

3.3.2. Experimental comparison results

This article uses the three indicators mentioned in section 3.1 and the results are shown in Table 1.

It can be seen that whether the accuracy, recall or precision of the method proposed in this article has been improved on several classic classifiers, indicating that the data augmentation method used in this article can effectively solve few problems related to the amount of data. This method uses a data augmentation model which is more suitable for classification tasks. At the same time, it uses a hyper sphere model based on the theory of multi-granularity-particle sphere computing to obtain a more accurate spatial measurement relationship, and we receive the result that the expanded data is more representative and relevant. Then the hyper sphere model eliminates the upper and lower bounds of a single sample, which is simple and efficient. After the experiment, we find that the execution speed is much higher than that of the traditional k-means algorithm, which makes the data augmentation process less expensive computationally, faster, and lower in storage. It can be used in a relatively short time. Small data sources make feasible and effective expansion. The method used in this paper introduces ball k-means algorithm's neighbor sphere clusters, the stable areas, convenient calculation, the feature of easy to understand, and strong interpretability.

Table 1 Experimental results

Data sets	Classifiers	AD	RD	PD
Four-class	SVM	0.0154	0.0414	0.0280
	NB	0.0386	0.0683	0.0051
	RF	-0.0040	-0.0034	-0.0010
Digits	SVM	0.0019	0.0018	0.0019
	NB	0.0740	0.0522	0.0744
	RF	-0.0019	0.0002	-0.0017
Iris	SVM	0.0002	0.0010	0.0003
	NB	-0.0067	-0.0076	-0.0109
	RF	-0.0023	-0.0046	-0.0106
Breast-cancer	SVM	0.0051	0.0091	0.0078
	NB	0.0117	0.0308	-0.0040
	RF	0.0176	0.0176	0.0205

4. Conclusions

The method in this paper consists of four modules in total: ball k-means cluster, data augmentation, data marker and classifier. In ball k-means cluster, the algorithm utilized this paper uses the method of dividing the stable area in order to efficiently and quickly find the most obvious regions of the data set; after finding the stable areas of the ball cluster, using the normal distribution in the stable areas can generate a large amount of strongly correlated data; then we add the expanded data as input, using purity to label it, and after that we obtain a large amount of completely labeled data. In this paper, the method expands the data set by combining ball k-means cluster, and makes a full use of the hyper sphere model and ball k-means idea. The method we proposed does not require manual extraction of processing features, which avoids a large scale of tedious data processing, and it reduces errors in manual selection. Experiments have proved that using the data augmentation method proposed in this paper for classification can provide higher accuracy and precision.

In the experiment, we can find that the method we use has problems because it is difficult to grasp the k value of different data sets and to converge to non-convex data sets. The next step of our study will be put on conducting research towards this problem. In order to improve the convergence ability of this method on non-convex data sets.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (No.62076042), the Key Research and Development Project of Sichuan Province (No.21SYSX0082, No. 2020YFG0307.

References

[1] K. Chatfield, K. Simonyan, A. Vedaldi, and A. Zisserman. “Return of the devilin the details:Delving deep into convolutional nets”. In British Machine Vision Conference, 2014.

[2] R. Mash, B. Borghetti, and J. Pecarina. “Improved aircraft recognition for aerial refueling through data augmentation in convolutional neural networks”. In International Symposium on Visual Computing, 2016.

[3] M. Zeiler and R. Fergus. “Visualizing and understanding convolutional networks”. In European Conference on Computer Vision, pages 818–833.Springer International Publishing, 2014.

[4] Luke Taylor, Geoff Nitschke. “Improving Deep Learning using Generic Data Augmentation”. In Computer Science, 2017.

[5] S. Xia et al., "A Fast Adaptive k-means with No Bounds," in IEEE Transactions on Pattern Analysis and Machine Intelligence, Chongqing, 2020.

ROLE OF MACHINE LEARNING IN HUMAN STRESS: A REVIEW

FAIJAN AKHTAR[1], MD BELAL BIN HEYAT[1], JIAN PING LI[1*], PARTH K. PATEL[2], RISHIPAL[3], BISHAL GURAGAI[3]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan 611731, China
[2]Department of Pharmacy, H.K. College of Pharmacy, Mumbai University, Jogeshwari, Mumbai, Maharashtra 400102, India
[3]School of Life Science and Technology, University of Electronic Science and Technology of China, Chengdu, 610054, China
E-MAIL: jpli2222@uestc.edu.cn

Abstract:

Stress is one type of epidemic of current world. It generates many diseases and is a big source of human suicide. The main aim of this paper is to determine the work of this study conducted on stress using emerging techniques such as machine learning. This study created a comprehensive image for the work of machine learning in stress management. This study completed in some steps including data collection using closest keywords on Web of Science (WoS) database, design network visualization based on previous data, evaluation of selected research article, and finally conclude the all results. We used 4 closest keywords, 5 research articles, 3 publishers, and 4 journals to analyze the work. The results showed that Support Vector Machine (SVM) easily classify the signals. This study mentioned the future direction for the upcoming research in more scientific and significant manner.

Keywords:

Detection; Machine learning; Prediction; Stress; SVM; Web of Science

1. Introduction

Stress is considered as a cancer of mind [1], it has been health epidemic of twenty first century [2]. Stress is considered to be one of the special characteristics of our life and everybody experiences it in their life as it is an inevitable aspect [3]. It is considered to be one amongst the foremost aspects of our current life, which has occasioned from the modernity and changes in human beings. Consequently, this period is known as age of stress [4]. Any event or factor that can cause actual or perceived threat to an organism and contribute to stress is called as 'stressor'[5-6]. Stressors can be of several types: life events, physiological or physical changes in body, environmental changes, and social influence. Sometimes imaginary situations tend to act as a stressor. Therefore our perceptions towards any event or situation play a major role in today's stressful life. Depending on the nature, influence of stress on individual and duration of exposure, stress can be categorized into various categories: Physiological stressors are also called as homeostatic or systemic stressors. These aims several physiological parameters, and their outcome is refereed through receptors system, viscera sensory pathways and directly affects stress-related motor neurons. It causes damage to body tissue and is indicated by an emotional experience. Psychological stressors are also known as emotional or neurogenic stimuli. This type of stress is encountered under situations arising due to social threats like social exclusion, evaluation and achievements situation. If the gratification of the needs like to maintain social-self, to get affiliated by others is threatened; for example getting negatively judged for a performance by others [7-8]. Acute stress is common in people that worry excessively and lives extremely busy and disorganized life. Generally the symptoms are irritability, anxiety, anger. If acute stress occurs frequently, it is termed as episodic stress. People face episodic stress when they encounter series of stressful challenges continuously one after the other. When stress remains for a longer period of time, it is termed as chronic stresses. Long term exposure to stressors can lead to chronic stress. It can severely affect the physical, emotional and psychological health. The effect of stress on body may vary from person to person depending upon several factors like age, sex, past experiences, physiological conditions, type of stress. Stress increases cortisol levels and affect the activity of insulin and thus shows negative effect on maintenance of blood glucose levels on type I and II both diabetic patients [6]. Chronic stress outcome in atrophy of mind and gradually reduction its weight over a period of time [9]. Stress hormones can cause vasodilation and raises blood pressure.

Therefore stress can worsen the condition of an individual who is suffering from diseases like asthma, emphysema [10]. It has been found from studies that stress mediators can exert their effects on the immune system by crossing the blood-brain barrier. Excessive stress reduces the activity of natural killer cells and cytotoxic T-lymphocytes in our body which allows growth of malignant cells and contribute to expansion of tumor [11].

Machine learning is a basically ability by which computer can learn by self without being especially program. It is the scientific study of statistical model and algorithms that computer system usages to complete a specific duty without using patterns, obvious instructions, and implication as an alternative. It is divided into four parts including supervised, unsupervised, semi supervised, and reinforcement machine learning. The many physiological signals are used in the detection, diagnosis, and prediction of the different diseases like heart diseases, mental disorders, skin disorders, and eye disorders [12-15]. *Lai, Siddiqui* and *Heyat group's* and used physiological signals and different machine learning classifiers to detect sleep disorders [16-25]. Machine learning methods opened the new way to easily detect, diagnose, predict, and calculate the risk of any diseases. This study provides an outline of the stress and use of machine learning methods in the stress management. Fig. 1 demonstrated the role of machine learning in assessing the stress of human.

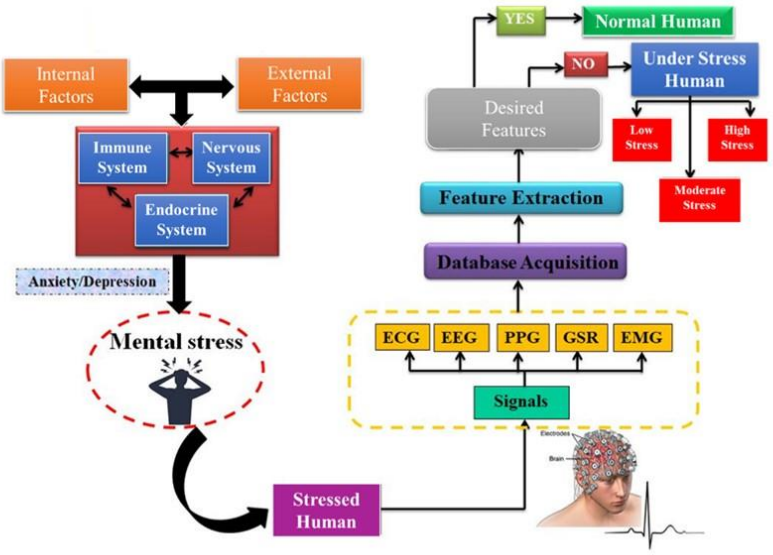
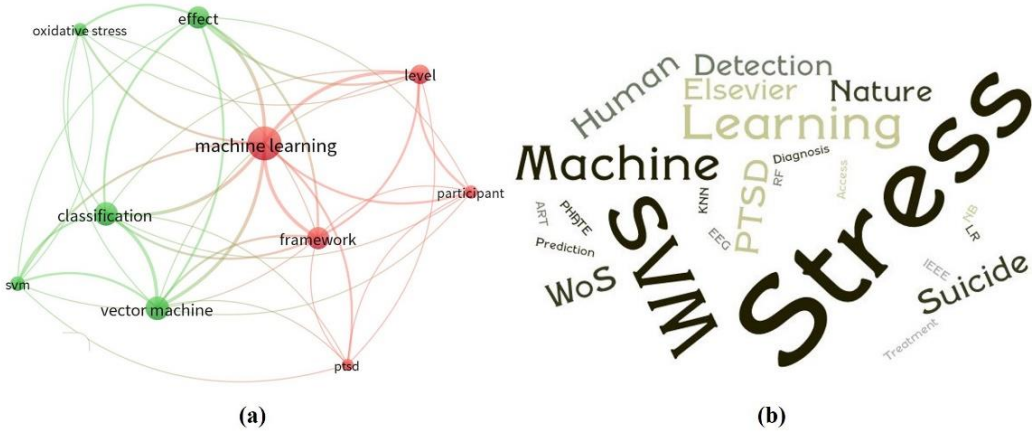


Fig.1 Role of machine learning in stress assessment.

2. Screening method

Publications were retrieved by accessing to Web of Science database by computerized search to collect the previous data related to the human stress. We applied this method TITLE: ("Stress") AND TITLE: ("Machine Learning") AND TOPIC: ("Human") AND TOPIC: ("Health") to find the exact result. Research articles written only in English were included in this study, whereas review articles, book chapter, abstract and other articles written in Spanish, Chinese, and Japanese language were excluded. We got eight articles for above method and after screening five articles which reported the best relevance for this study were selected. The selected papers are indexed in various popular databases such as WOS, DIIDW, KJD, MEDLINE, RSCI, and SCIELO.



(a) (b)

Fig.2 Comprehensive image of the (a) network visualization and (b) word cloud as of this study.

Table 1 Previously published article based on closest keywords such as stress, machine learning, human and health.

Author	Year	Major	Classifier	Objective	Journal Name	Publisher
Zhang et al. [26]	2020	PHATE, MI	KNN, RF, SVM	Protection	Analytica Chimica Acta	Elsevier
Zhang et al. [27]	2020	MEG, EEG wave	SVM	Diagnosis	Scientific Reports	Nature
Dubey et al. [28]	2019	ART	SVM	Treatment	Scientific Reports	Nature
Papini et al. [29]	2018	Medical features, Demographic features	LR	Prediction	Journal of Anxiety Disorders	Elsevier
Subhani et al. [30]	2017	T-test, Bhattacharya distance	LR, SVM, NB	Detection	IEE Access	IEEE

PHATE: Potential of Heat-diffusion for Affinity-based Transition Embedding; MI: Mutual Information; KNN: K-Nearest Neighbor; RF: Random Forest; SVM: Support Vector Machine; MEG: Magnetoencephalography; ART: Assisted Reproductive Technology, LR: Logistic Regression

3. Discussion

In Table 1, we evaluate the five research articles based on author, year, major, classifier, objective, journal, and publication house. Additionally, the Fig. 2 (a) and Fig. 2 (b) represented the network visualization [31]-[34] and world cloud of this study, respectively. Previously, *Zhang et al.* [26] used novel Potential of Heat-diffusion for Affinity-based Transition Embedding (PHATE) and Mutual Information (MI) techniques to imagine the data of Raman spectral. They used KNN, RF, and SVM machine learning classifiers for the analysis, effectiveness, and treatment of the oxidative stress. *Zhang et al.* [27] used EEG and MEG wave to detect the Post Traumatic Stress Disorder (PTSD) using SVM supervised machine learning classification. They used 23 subjects and extracted EEG waves such as theta, gamma, alpha, and beta as a feature extraction and classify the signals using SVM classifier on MEG signals. *Dubey et al.* [28] studied that Assisted Reproductive Technology (ART) used for the counting of sperm cell and treatment of infertility. They used SVM and achieved 91.18 % sensitivity of the system. *Papini et al.* [29] used hospital and demographic features for the prediction of stress using LR classifier. *Subhani et al.* [30] extracted Bhattacharya distance as features and discriminate the control and stress group using different classifiers such as LR, SVM, and NB.

4. Conclusions

Globally, stress is one of the health epidemics of 21st century. Consequently, it is essential to control and monitor of stress, to prevent the harmful consequences in future. We obtained that SVM would be helpful in the detection and prediction of stress disorder. In addition, several emerging techniques such as unsupervised machine learning, deep learning methods, quantum techniques, and block chain technology can be of great importance to diagnose, and predict the stress with high accuracy.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, the project of Science and Technology Department of Chongqing Municipality, Chengdu Chengdian Network Technology Co., Ltd., Chengdu Civil-military Integration Project Management Co., Ltd., and Sichuan Yin Ten Gu Technology Co., Ltd. We also acknowledge to school coordinator, Prof. Naseem, Syed Shafqat Ali, Dr. Lari, and Miss Mariyam Hashmi for the support and help.

References

[1] Q. Bukhsh, A. Shahzad, and M. Nisa, "A study of learning stress and stress management strategies of the students of postgraduate level: A case study of Islamia university of Bahawalpur, Pakistan," *Procedia - Soc. Behav. Sci.*, vol. 30, pp. 182–186, 2011.

[2] G. Fink, "Stress: Definition and history," Reference Module in Neuroscience and Biobehavioral Psychology. pp. 1–9, 2017.

[3] A. M. Shahsavarani, E. Azad, M. Abadi, and M. H. Kalkhoran, "Stress: Facts and Theories through Literature Review," Int. J. Med. Rev., vol. 2, no. 2, pp. 230–241, 2015.

[4] S. G. Yahya, Farzan, Kashif Ud Din Khan, "Crucial Factors Affecting Stress : a Study Among undergraduates in Pakistan," Int. J. Asian Soc. Sci. J., vol. 3, no. 2, pp. 428–442, 2013.

[5] N. Schneiderman, G. Ironson, and S. D. Siegel, "Stress and health: Psychological, behavioral, and biological determinants," Annu. Rev. Clin. Psychol., vol. 1, pp. 607–628, 2005.

[6] D. K. Sharma, "Physiology of Stress and its Management," J. Med. Study Res., vol. 1, no. 1, pp. 1–5, 2018, doi: 10.24966/msr-5657/100001.

[7] L. Kogler et al., "Psychosocial versus physiological stress – meta-analyses on deactivations and activations of the neural correlates of stress reactions," Neuroimage, vol. 1, no. 119, pp. 235–251, 2016.

[8] K. J. Kovács, I. H. Miklós, and B. Bali, Psychological and physiological stressors, vol. 15. 2005.

[9] H. Yaribeygi, Y. Panahi, H. Sahraei, T. P. Johnston, and A. Sahebkar, "The impact of stress on body function: A review," EXCLI Journal. 2017.

[10] D. K. N. S. Borikar, Hiral, "Stress and Human Body System Reaction – A Review," Int. Multidiscip. Res. J., vol. 3, no. 12, pp. 1–6, 2016.

[11] H. Yaribeygi, Y. Panahi, H. Sahraei, T. P. Johnston, and A. Sahebkar, "stress can decrease the activity of cytotoxic T lymphocytes and natural killer cells and lead to growth of malignant cells, genetic instability, and tumor expansion," EXCLI J., vol. 16, pp. 1057–1072, 2017.

[12] B. Bin Heyat, Y. M. Hasan, and M. M. Siddiqui, "EEG signals and wireless transfer of EEG Signals," Int. J. Adv. Res. Comput. Commun. Eng., vol. 4, no. 12, pp. 10–12, 2015.

[13] M.B.B. Heyat and M. M. Siddiqui, "Recording of EEG, ECG, EMG Signal," vol. 5, no. 10, pp. 813–815, 2015,

[14] D. Lai, X. Zhang, Y. Zhang, and M. B. Bin Heyat, "Convolutional Neural Network Based Detection of Atrial Fibrillation Combing R-R intervals and F-wave Frequency Spectrum," 2019, doi: 10.1109/EMBC.2019.8856342.

[15] D. Lai, Y. Zhang, X. Zhang, Y. Su, and M. B. Bin Heyat, "An Automated Strategy for Early Risk Identification of Sudden Cardiac Death by Using Machine Learning Approach on Measurable Arrhythmic Risk Markers," IEEE Access, 2019.

[16] D. Lai, M. B. Bin Heyat, F. I. Khan, and Y. Zhang, "Prognosis of Sleep Bruxism Using Power Spectral Density Approach Applied on EEG Signal of Both EMG1-EMG2 and ECG1-ECG2 Channels," IEEE Access, vol. 7, pp. 82553–82562, 2019, doi: 10.1109/ACCESS.2019.2924181.

[17] M. B. Bin Heyat, D. Lai, F. I. Khan, and Y. Zhang, "Sleep Bruxism Detection Using Decision Tree Method by the Combination of C4-P4 and C4-A1 Channels of Scalp EEG," IEEE Access, vol. 7, pp. 102542–102553, 2019.

[18] M. B. Bin Heyat et al., "A Novel Hybrid Machine Learning Classification for the Detection of Bruxism Patients Using Physiological Signals," Appl. Sci., vol. 10, 2020, doi: 10.3390/app10217410.

[19] M. B. B. Heyat, F. Akhtar, M. Ammar, B. Hayat, and S. Azad, "Power Spectral Density are used in the Investigation of insomnia neurological disorder," in XL- Pre Congress Symposium, 2016, pp. 45–50.

[20] M.B.B Heyat, F. Akhtar, M. Sikandar, H. Siddiqui, and S. Azad, "An Overview of Dalk Therapy and Treatment of Insomnia in Dalk Therapy Abstract- Treatment of Insomnia in Dalk Therapy," 2015.

[21] M.B.B. Heyat, F. Akhtar, A. Mehdi, S. Azad, S. Azad, and S. Azad, "Normalized Power are used in the Diagnosis of Insomnia Medical Sleep Syndrome through EMG1-EMG2 Channel," Austin J. Sleep Disord., vol. 4, no. 1, pp. 2–4, 2017.

[22] M. B. Bin Heyat, F. Akhtar, and S. Azad, "Comparative

Analysis of Original Wave and Filtered Wave of EEG signal Used in the Prognostic of Bruxism medical Sleep syndrome," Int. J. Trend Sci. Res. Dev., vol. Volume-1, no. Issue-1, pp. 7–9, 2016, doi: 10.31142/ijtsrd53.

[23] M. B. Bin Heyat, Insomnia: Medical Sleep Disorder & Diagnosis, 1st ed. Hamburg, Germany: Anchor Academic Publishing, 2016.

[24] B. Bin Heyat, F. Akhtar, S. K. Singh, and M. M. Siddiqui, "Hamming Window are used in the Prognostic of Insomnia," in International Seminar Present Scenario Future Prospectives Res. Eng. Sci. (ISPSFPRES), 2017, pp. 65–71.

[25] M. B. Bin Heyat et al., "Detection, Treatment Planning, and Genetic Predisposition of Bruxism: A Systematic Mapping Process and Network Visualization Technique," CNS Neurol. Disord. - Drug Targets, 2020.

[26] W. Zhang et al., "Label-free discrimination and quantitative analysis of oxidative stress induced cytotoxicity and potential protection of antioxidants using Raman micro-spectroscopy and machine learning," Anal. Chim. Acta, 2020, doi: 10.1016/j.aca.2020.06.074.

[27] J. Zhang, J. D. Richardson, and B. T. Dunkley, "Classifying post-traumatic stress disorder using the magnetoencephalographic connectome and machine learning," Sci. Rep., 2020.

[28] V. Dubey et al., "Partially spatially coherent digital holographic microscopy and machine learning for quantitative analysis of human spermatozoa under oxidative stress condition," Sci. Rep., 2019.

[29] S. Papini et al., "Ensemble machine learning prediction of posttraumatic stress disorder screening status after emergency room hospitalization," J. Anxiety Disord., 2018, doi: 10.1016/j.janxdis.2018.10.004.

[30] A. R. Subhani, W. Mumtaz, M. N. B. M. Saad, N. Kamel, and A. S. Malik, "Machine learning framework for the detection of mental stress at multiple levels," IEEE Access, 2017, doi: 10.1109/ACCESS.2017.2723622.

[31] M.B.B. Heyat et al., "Progress in Detection of Insomnia Sleep Disorder: A Comprehensive Review," Curr. Drug Targets, 2020.

[32] F. Akhtar et al., "Potential of Blockchain Technology in Digital Currency: A Review," in 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, 2019, pp. 85–91.

[33] N. J. van Eck and L. Waltman, Measuring Scholarly Impact: Methods and Practice. 2014.

[34] N. J. van Eck and L. Waltman, "Visualizing Bibliometric Networks," in Measuring Scholarly Impact, 2014.

ANALYSIS AND EVALUATION OF HOUSING PRICE FOR CHENGDU URBAN

MU-JIE LI[1,2], MING-CANG ZHU[3], YONG HE[4], PENG-SHAN LI[5], XIAO-BO ZHANG[6], ZHAN-YONG HE[4], JI-BAO SHI[6], KAI CHEN[6], TAO WENG[6], ZE-ZHONG ZHENG[1,2]*, LING JIANG[1,2]*

[1]Key Laboratory of Urban Land Resources Monitoring and Simulation, Ministry of Land and Resources, Shenzhen, Guangdong, PRC 518040
[2]School of Resources and Environment, University of Electronic Science and Technology of China, Chengdu, Sichuan, PRC 611731
[3]Department of Natural Resources of Sichuan Province, Chengdu, Sichuan, PRC 610072
[4]Sichuan Research Institute for Eco-system Restoration & Geo-disaster Prevention, Chengdu, Sichuan, PRC 610081
[5]Chengdu Land Planning and Cadastre Center, Chengdu, Sichuan, PRC 610074
[6]Chengdu Institute of Survey & Investigation, Chengdu, Sichuan, PRC 610081
E-MAIL: zezhongzheng@uestc.edu.cn.

Abstract:

House prices have received unusual attention in recent years, and evaluation of housing price has also become a research hotpot. Value of a house is considered as a mixture of various features, such as house type, orientation and location. Accurate assessment of houses thus faces a large number of challenges. Several methods have been applied to assess the value of a house, including geographically weighted regression and machine learning. However, every method has some limitations. The accuracy of traditional regression methods needs to be improved. Machine learning methods are weak in interpretability. In this paper, to analyze the housing price, we compared XBGoost, Random Forest, Support vector regression, back-propagation network and geographically weighted regression to model the second-hand housing price dataset, and analyzed the influenced of each feature. The result shows Random Forest reaches a lowest mean absolute error of 1517.29 and best r2 of 0.83. According to the constructed models, the importance values are given, and the area of house shows a strongest influence on housing price in the study area.

Keywords:

Housing price; Influencing factors; Machine Learning; Geographically Weighted Regression

1. Introduction

In the past decade, there has been a dramatic increase in house prices in China. Government, social and individual pay close attention to the influencing factors of housing price and try to study the law of change in housing price. Researchers have proposed several theories to study the influencing factors of housing price change. Hedonic pricing method [1] is one of the main methods in this field. Jim and Chen [2] utilized hedonic pricing method to explore the impacts of key environmental elements on residential housing value, including window orientation, green-space view, floor height, proximity to wooded areas and water bodies, and exposure to traffic noise. Huang and Yin [3] used hedonic price models to examine a comprehensive set of environmental sustainability elements and compare their relative importance. However, these studies of housing price influencing factors usually predict the housing price with a low accuracy.

Great progress has been made in deep learning research and machine learning. And researchers applied deep learning and machine learning to predict housing price. Limsombunchai [4] utilized artificial neural network to predict the housing price based on the samples downloaded from the Internet, and verified the feasibility of artificial neural network in the housing price prediction. Wang et al. [5] proposed a house price prediction method based on particle swarm optimization and support vector machine, which achieved good results. Due to the characteristics of algorithms, these methods are weak in interpretability.

In the paper, we constructed a dataset by merging the point of information (POI) data and dataset of second-hand housing price download from Internet, applied eXtreme Gradient Boosting (XGBoost) [6], Random Forest, Support vector regression, back-propagation network and geographically weighted regression (GWR) [7] to model the second-hand housing price. At last, influencing factors of housing price are analyzed, and an accurate valuation model was constructed.

2. Methods

In order to obtain a sufficient amount of dataset, we firstly crawled second-hand housing transaction data on the real estate exchange website, and collected POI data of Chengdu city. By data cleaning and data fusion, a housing price dataset was generated. Then, we tested several methods to model the dataset, and gained the priority of feature importance. Finally, an accurate valuation model was constructed. The technical flow chart of this study is shown in Fig. 1.

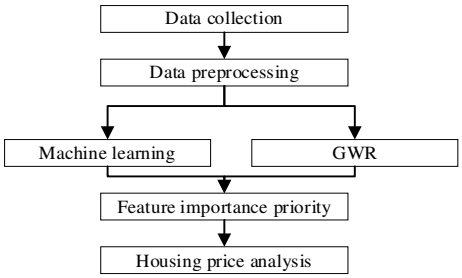


Fig.1 Flow chart of this paper

2.1. Data preprocessing

Data utilized in this paper consist of two parts. The first part mainly contains house property scrawled from the real estate transaction website - fang.com. There are duplicate values and error values in the raw data, thus, data cleaning was performed. The second part was extracted from the POI data. Distance between each house and various points of information was calculated

2.2. Machine learning

XGBoost and random forest are applied in this paper. XGBoost are based on tree boosting, and it was widely used in Kaggle and presented an excellent performance. Random forest is also based on the ensemble learning and unexcelled in accuracy among current algorithms. XGBoost and random forest can give estimates of variable importance, which assists the analysis of housing price features.

2.3. GWR

The main idea of the hedonic model is to disaggregate the price in order to highlight the implied price of the influential feature. Hedonic price model can generally be expressed by the formula (1) [1].

$$P = C_0 + \sum_i C_i X_i + \varepsilon \quad (1)$$

Where, P represents the price, C0 is the intercept, Ci is the weight of the i^{th} feature Xi, ε presents the error.

With the development of hedonic model, GWR was proposed to consider the influence of spatial position on the weight of each feature. GWR [7] can be presented as the formula (2).

$$y_i = \beta_0(u_i, v_i) + \sum_{k=1}^{p} \beta_k(u_i, v_i) x_{ik} + \varepsilon_i \quad (2)$$

Where, y_i represents the price of i^{th} sample; (u_i,v_i) denotes the location information of i^{th} sample. $\beta_k(u_i,v_i)$ denotes the weight in the i^{th} location; x_{ik} is the k^{th} feature in the i^{th} location; ε_i presents the error in the i^{th} location. $\beta_k(u_i,v_i)$ can be calculated by weighted least squares(WLS), and the following objective function (3) is constructed.

$$\min \sum_{j=1}^{n} w_j(u_i, v_i)(y_i - \beta_0(u_i, v_i) - \sum_{k=1}^{p} \beta_k(u_i, v_i) x_{ik})^2 \quad (3)$$

Where, $w_j(u_i,v_i)$ represents a monotonically decreasing function of distance d_{ij}, and generally calculated by Gaussian kernel function (4) or Bi-square kernel function (5) [8].

$$W_{ij} = \exp[(-d_{ij}^2/h^2)] \quad (4)$$

$$W_{ij} = \begin{cases} \left[\left(-\frac{d_{ij}^2}{h^2}\right)\right] & d_{ij} \le h \\ 0 & d_{ij} > h \end{cases} \quad (5)$$

Where, h denotes bandwidth that can be calculated by cross validation (CV) or Akaike information criterion (AIC).

2.4. Performance Metrics

The R squared(R^2), Root Mean Squard Error (RMSE), Mean Absolute Error (MAE) are adopted as performance metrics in this study [9].

$$R^2 = 1 - \frac{\sum_i (\hat{y}_i - y_i)^2}{\sum_i (\bar{y} - y_i)^2} \quad (6)$$

$$\mathrm{RMSE} = \sqrt{\frac{1}{m}\sum_{i=1}^{m}(y_i - \hat{y}_i)^2} \quad (7)$$

$$\mathrm{MAE} = \frac{1}{n}\sum_{i=1}^{n} |\hat{y}_i - y_i| \quad (8)$$

Where, $\hat{y}_i$ denotes the predicted value; $y_i$denotes the true value; $\bar{y}$ denotes the mean value.

3. Experiments

3.1. Data

In this study, Qingyang and Wuhou districts were selected as the study area. Data utilized in this paper consist of two parts. The first part was scrawled from the real estate transaction website, including, number of bedrooms, number of living rooms, number of bathrooms, area, orientation, floors, decoration, building age, elevator, building category,

residential category, green rate, floor area ratio, total number of buildings, total number of households. The second part consist of longitude, latitude, school distance, bus distance, subway distance, hospital distance, number of nearby commercial facilities, number of enterprises, cultural facilities distance, entertainment facilities distance, enterprise distance. In this study, after data preprocessing, 9,986 house samples are contained in the dataset.

3.2. Models Setting

Feature selection was performed by using backward selection. In order to ensure the calculation of the GWR model, the dummy variables were deleted.

The parameters of the machine learning model were selected using grid search and cross validation. Based on the dataset, the Bi-square kernel function was used to build the GWR model, and the CV method was used to select the optimal bandwidth. For the BP network, we adjusted the depth of different hidden layers and the number of neural nodes, the structure utilized in this study is input (25) - (200 *5) - (300 *5) - (256 *5) - (128 *2) - (64) - (16)-output. Adam was selected as the optimizer, and ReLu was selected as the activation function.

4. Result

In this study, 5-fold cross-validation was adopted to evaluate the models. Table 1 shows the result of the models.

Table 1 Models test results

Methods	R2	RMSE(yuan/m^2)	MAE(yuan/m^2)
XGBoost	0.81	2610.76	1577.34
RF	0.83	2454.02	1517.29
SVR	0.744	3021.45	1935.51
GWR	0.74	3067.72	2001.51
BP	0.66	3299.9	2160.60

The experiments result indicated that RF reached the best performance, R squared reaches 0.824, RMSE is calculated as 2501.39, and MAE is 1585.17. The result of XGBoost is close to that of RF, while the other model results are not ideal.

XGBoost and RF give a ranking of feature importance. Figure 2 shows the importance value given by XGBoost.

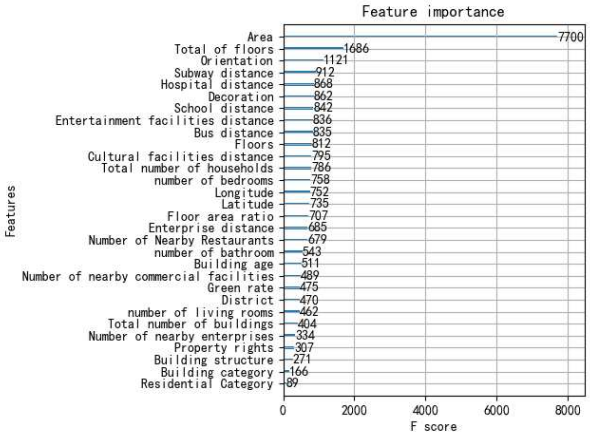


Fig.2 Feature importance

The top 10 most important features given by random forests are: Area, Total of floors, Building age, Cultural facilities distance, Latitude, number of bathroom, number of bedrooms, Number of Nearby Restaurants, Longitude, District, Hospital distance, Total number of households, Number of nearby commercial facilities, Floor area ratio, Enterprise distance, Subway distance, Entertainment facilities distance, Bus distance, School distance, Number of enterprises, Total number of buildings, number of living rooms, Green rate, Decoration, Orientation, Floors, Building category, Building structure, Property rights, Residential Category.

$\beta_k(u_i,v_i)$ was calculated by GWR model. Statistical result of the weight of partial features was showed as fellow.

Table 2 Statistics of GWR model weight

Feature	Mean	STD	MIN	Median	MAX
Building age	2438.455	1397.978	-2392.182	2618.344	6195.516
No. commercial facilities	1929.621	4752.543	-80385.953	1703.028	42982.106
Longitude	-1377.382	11828.654	-48532.682	-3815.355	60055.034
Cultural facilities distance	-1295.555	5045.766	-14619.033	-1876.9	17431.744
No. Restaurants	-1034.517	2496.484	-8933.623	-821.44	14723.41
Entertainment facilities distance	-918.737	1677.666	-10719.267	-821.61	4677.878
No. bathroom	583.34	600.784	-5475.864	654.52	2533.403
Enterprise distance	547.02	1073.764	-2999.589	479.113	7699.993
Floor area ratio	-513.719	1490.042	-9489.68	-175.269	20296.82
No. bedrooms	476.399	1002.29	-4226.392	674.285	2149.558
Green rate	-373.321	690.373	-2844.811	-209.549	834.148

5. Discussion

As can be seen from the results, XBGoost and RF, as current cutting-edge machine learning algorithms, both perform high fitting effects. The BP neural network is different from the ensemble tree algorithm. Simple back-propagation training performs poorly in this dataset, and its applicability is not as good as XGBoost and RF. Although GWR result shows a low metrics, it is more explanatory and show spatial non-stationarity.

According to the feature importance evaluation and feature weights given by the models, we can see that area of a house has the strongest impact on housing prices. Distance between house and public facilities and the number of public facilities also received a high importance evaluation. It can be inferred that consumers in the study area value the convenience of transportation and the integrity of surrounding facilities. Government could optimize the transportation and infrastructure construction in the area.

6. Conclusions

In this study, we scrawled 9 987 house samples with 15 house properties and extracted 9 features from POI data which contains a wealth of public facilities information. Then, a dataset of housing price was obtained after data preprocessing. Both machine learning methods and the traditional GWR model are tested in the study, and we obtained the feature importance assessment given by the models. The results show that cutting-edge models such as XGBoost and RF perform significantly better than traditional BP networks and GWR models. RF reached a result that R squared is 0.83, RMSE is 2454.02 and MAE reaches 1 517.29. Among all the features, the area and distance features have a strong influence on the housing price.

Acknowledgements

The work was supported in part by the Open Fund of Key Laboratory of Urban Land Resources Monitoring and Simulation，Ministry of Natural Resources (Grant No. KF-2019-04-074, Grant No. KF-2019-04-069, and Grant No. KF-2018-03-063); Open Fund of State Key Laboratory of Water Resources and Hydropower Engineering Science (Grant No. 2014SWG04, and Grant No.2018SWG02); Science Research Program of Natural Resources Department of Sichuan Province (Grant No. KJ-2020-3); and Opening Foundation of Guangxi Key Laboratory for Spatial Information and Geomatics, Guangxi, China (Grant No. 17-259-16-14 and Grant No. 19-050-11-06), The Key Technologies Research and Development Program of Sichuan Province (Grant No. 2020YFSY0041).

References

[1] Ozalp. A. Y, and Akinci. H, “The use of hedonic pricing method to determine the parameters affecting residential real estate prices”, Arabian Journal of Geosciences, Vol 10, No. 24, pp.535. 2017.

[2] Jim. C. Y, and Chen. W. Y, “Impacts of urban environmental elements on residential housing prices in Guangzhou (China)”, Landscape and Urban Planning, Vol 78, No. 4, pp. 422-434. 2006.

[3] Huang. H, and Yin. L, “Creating sustainable urban built environments: An application of hedonic house price models in Wuhan, China”, Journal of Housing and the Built Environment, Vol 30, No. 2, pp. 219-235. 2015.

[4] Limsombunchai. V, “House price prediction: Hedonic price model vs. artificial neural network”, New Zealand Agricultural and Resource Economics Society Conference, Blenheim, pp. 25-26, 2004.

[5] Wang X, Wen J, Zhang Y, et al., “Real estate price forecasting based on SVM optimized by PSO”, Optik-International Journal for Light and Electron Optics, Vol 125, No. 3, pp. 1439-1443. 2014.

[6] Chen. T, and Guestrin. C, “Xgboost: A scalable tree boosting system.”, In Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining, San Francisco, pp. 785-794. August, 2016

[7] Brunsdon, C, Fotheringham. A.S, and Charlton. M. E, “Geographically weighted regression: a method for exploring spatial nonstationarity.”, Geographical analysis, Vol 28, No. 4, pp.281-298. 1996.

[8] Mohammadinia. A, Alimohammadi. A, and Ghaemi. Z, “Evaluation and Comparison of Performance of Fixed and Adaptive Kernels in Geographically Weighted Regression for Modeling Leptospirosis in Gilan.”, Journal of Geomatics Science and Technology, Vol 7, No. 3, pp.57-73. 2018

[9] Shahabi. M, Jafarzadeh. A. A, Neyshabouri. M. R, Ghorbani. M. A, and Valizadeh. Kamran. K, “Spatial modeling of soil salinity using multiple linear regression, ordinary kriging and artificial neural network methods.”, Archives of Agronomy and Soil Science, Vol 63, No. 2, pp.151-160. 2017.

CLASSIFICATION OF SURFACE NATURAL RESOURCES BASED ON U-NET AND GF-1 SATELLITE IMAGES

MU-JIE LI[1,2], MING-CANG ZHU[3], ZHIGANG MA[4], PENG-SHAN LI[5]*, XIAO-BO ZHANG[6], AN-KAI HOU[1,2], JI-BAO SHI[6], YONG HE[4], KAI CHEN[6], TAO WENG[6], ZHAN-YONG HE[4], ZE-ZHONG ZHENG[1,2]*, LING JIANG[1,2]

[1]Key Laboratory of Urban Land Resources Monitoring and Simulation, Ministry of Land and Resources, Shenzhen, Guangdong, PRC 518040
[2]School of Resources and Environment, University of Electronic Science and Technology of China, Chengdu, Sichuan, PRC 611731
[3]Department of Natural Resources of Sichuan Province, Chengdu, Sichuan, PRC 610072
[4]Sichuan Research Institute for Eco-System Restoration & Geo-disaster Prevention, Chengdu, Sichuan, PRC 610081
[5]Chengdu Land Planning and Cadastre Center, Chengdu, Sichuan, PRC 610074
[6]Chengdu Institute of Survey & Investigation, Chengdu, Sichuan, PRC 610081
E-MAIL: targetlps@163.com.

Abstract:

Natural resources are indispensable for human survival and the protection and management of surface natural resources become more and more important. At present, remote sensing and deep learning approaches are using in land use and land cover area. In this paper, a U-Net model is developed to classify surface natural resources using GF-1 satellite images by semantic segmentation. Experiment results indicate the effectiveness of the U-Net model to segment the surface nature resources, which can be applied in practice to support the management of nature resources.

Keywords:

Surface natural resources; U-Net model; GF-1 satellite images; Semantic segmentation

1. Introduction

Land use and land cover (LULC) is one of the most useful research directions of remote sensing and nature resource is one hot area. The total amount of natural resources in China is large, and there are many kinds of them. However, the per capita amount of natural resources is small, and it is difficult to develop them. Therefore, the protection and management of natural resources are becoming more and more important. Common machine learning models, like support vector machine (SVM) [1], and extremely randomized trees (ERT) are often used to classify LULC and nature resources based on low resolution remote sensing images.

But with the rapid growth of remote sensing satellites, high-resolution remote sensing data plays an increasingly important role in land use area, and has been proved to be the most direct and effective method [2]. Gaofen-1 (GF-1) satellite is the first satellite of China's high-resolution earth observation system. And it is equipped with two 2-m resolution panchromatic/8-m resolution multispectral cameras and four 16-m resolution multispectral cameras. Three satellite include GF-1 satellite had been used for vegetation coverage retrieval and GF-1 got a good result [3]. The complexity of the forms and structures of a green space system was studied based on the GF-1 satellite data [4]. These studies prove that the high-resolution remote sensing image like GF-1 satellite could help the surface natural resources research.

In order to best use the high-resolution remote sensing image, many researchers have tried many deep learning methods to improve the accuracy compared with traditional methods. Deep learning method could find the knowledge hidden in the big data and tell us information by images [5]. And deep learning models have been improved a few times. Liu et al took an object-based image analysis method, fully convolutional networks (FCN) for enhancing classification of LULC [6]. Liu et al proposed a random filter pruning method based on residual neural network (ResNet) to improve classification performance [7]. And Han et al utilized U-Net model in land cover classification and prove the model is effective [8].

So in this paper, we propose the U-Net model into surface natural resources classification. The model is helpful to distinguish the different surface natural resources and also part the land use categories not resource. At the same time, we compare the result of the images with three channels, which are red (R) channel, green (G) channel and blue (B)

channel and four channels, which the another one is near infrared (NIR).

2. Methods

2.1. Study Area

The Pidu district of Chendu city of China is our study area, which is bounded by longitudes from 103° 42′ 50″ to 104° 2′ 29″ (E) and latitudes from 30° 43′ 13″ to 30° 52′ 39″ (N). We collected the GF-1 satellite image contain Pidu district and according to the administrative division, we cut it to get the Pidu image shown in Figure 1.

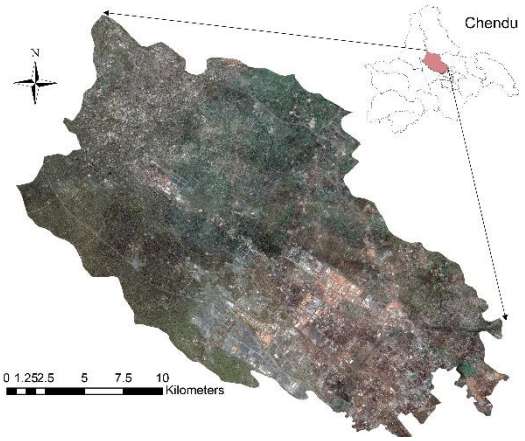


Fig.1 Pidu district image

2.2. System Diagram

The flowchart of our approach for surface nature resources classification is presented in Figure 2. First, we collected the GF-1 satellite image contain Pidu district, census data of geographical conditions and the administrative division of Chendu city. Then we cut the census data and image to get the Pidu district information for the next step. Second, according to the Pidu census data of geographical conditions, we labeled them into eight categories, which are woodland, water surface, field, building, flower nursery, road, grassland and others. Then we get the Pidu district 3-band image, 4-band image and its labeled image as two datasets. Third, we cut the datasets into 5000 images, 256×256 pixels and divided the datasets according to the ratio 3:1 of training sets and validation datasets. Finally, we took the two datasets to train two U-Net models and compared the results with overall accuracy (OA) and F1-Score.

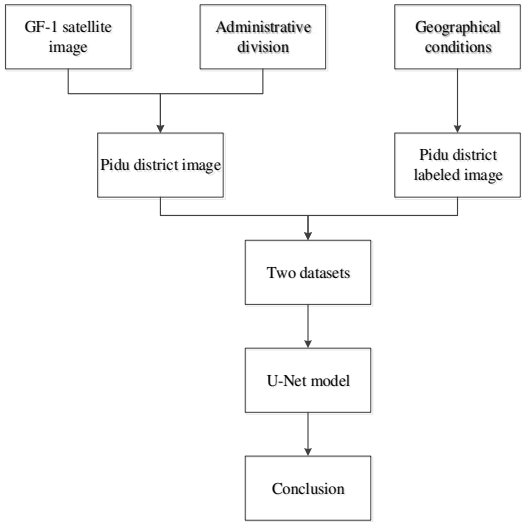


Fig.2 Flowchart of surface nature resources classification

2.3. U-Net

Semantic segmentation of image is to let the computer segment the image according to the semantic meaning of the image and U-Net is a commonly used network of it. The U-Net structure used in this paper is shown in Figure 3. The first left part is feature extraction as an encoder. The right part is the upper sampling part as a decoder. Since the network structure is like the shape of U, it is called U-Net network.

In the first left part, each pool layer has a scale, including the scale of the initial image, with a total of 5 scales. It realizes the multi-scale feature recognition of the image. In the second right part, each up-sampling and the number of channels corresponding to the feature extraction part are fused at the same ratio. It keeps image details of the feature extraction part.

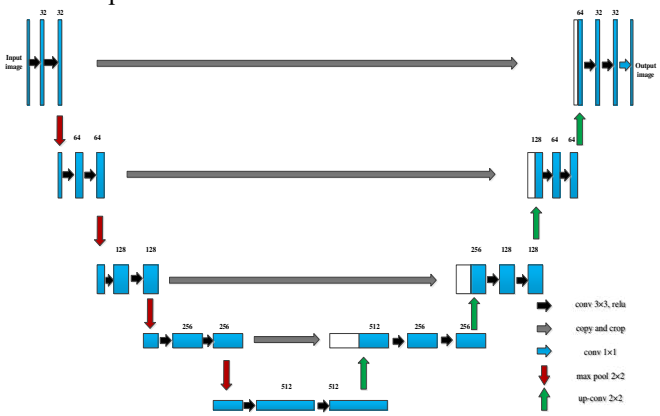


Fig.3 Structure of the U-Net

2.4. Performance Metrics

- Overall accuracy (OA)

OA is the ratio of the model's correct prediction to the overall number on all test sets. It is defined as

$$\mathrm{OA} = \frac{\sum n_i}{N} \quad (1)$$

Where n_i represents the correct prediction number of the i^{st} category, and N represents the overall number of all data.

- F1-Score

F1-Score is called balanced F-Score, and is defined as the harmonic average of precision and recall.

The precision formula is

$$\mathrm{precision} = \frac{TP}{TP+FP} \quad (2)$$

where TP represents the true prediction number of the category, and FP represents the number of other categories predicted as the category.

The recall formula is

$$\mathrm{recall} = \frac{TP}{TP+FN} \quad (3)$$

where TP represents the true prediction number of the category, and FN is the category number predicted as other categories.

The F1-score formula is

$$\mathrm{F1-score} = 2 \times \frac{precision \times recall}{precision + recall} \quad (4)$$

3. Experiments and Results

3.1. Training of U-Net model

We cut the datasets of 3-band image and 4-band image with their labeled images into 5000 images randomly. Each image is sized as 256×256 pixels. And we divided the datasets according to the ratio 3:1 of training sets and validation sets. The training sets are to train the U-Net models and the validation sets are to test the models' accuracy. And we got the best models with high validation accuracy as comparison.

3.2. Results of experiments

The results of two models are described in Figure 4. The picture (a) is chosen as a showcase in Pidu district, (b) is the labeled image of the showcase, (c) is the result of the U-Net model with 3-band input, (d) is the result of the U-Net model with 4-band input and (e) is the legend of these labeled images.

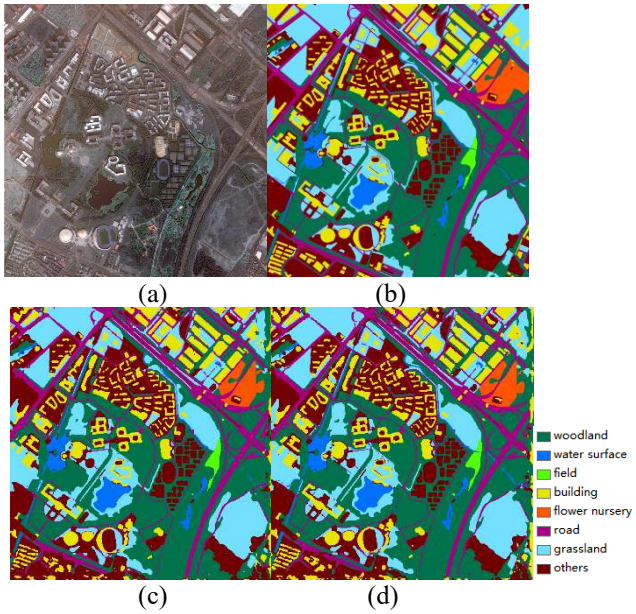


Fig.4 The results of two models

Table 1 The metrics results of models

Structure	OA (%)	F1-score (%)
U-Net with 3-band input	91.21	90.59
U-Net with 4-band input	91.72	91.23

From the picture c and d in figure 4, we could see the most pixels are correct divided and the outlines of the buildings are roughly unchanged.

And the metrics results of different structures are described in Table 1. It can be seen from the Table 1 that the result of U-Net model with 4-band input is better than 3-band input and they both get a good accuracy in surface nature resources classification. The U-Net model with 4-band input have the NIR channel as the input which could distinguish vegetation between building and others. So, we think the NIR channel make a great contribution for the U-Net model training.

Also, we analyzed the different classes without others of the best U-Net model and the results are described in Table 2.

It can be seen from the Table 2 that the surface nature resources like woodland, water surface and grassland could get good accuracy more than 92% of F1-score and this tell us U-Net model does effectively divide them. But the building, flower nursery and road have got lower accuracy which are planted and built and they are not surface nature resources. These classes are not the interest areas in this study. So, these results could meet the needs of the experiment and further research.

Table 2 The results of different classes in the best U-Net model

	Woodland	Water surface	Field	Building	Flower nursery	Road	Grassland
Precision(%)	91.90	91.82	94.30	89.98	96.21	88.14	94.21
Recall(%)	94.26	94.60	97.31	95.28	76.08	84.75	91.03
F1-score(%)	93.06	93.19	95.78	92.55	84.97	86.42	92.60

4. Conclusions

In this paper, we introduced U-Net model to classify surface nature resources, and chose woodland, water surface, field, building, flower nursery, road, grassland and others as our labels. From the results, we could see the model could get a good accuracy and effectively divide surface natural resources and the results could meet the needs of the experiment and further research. Also, the results showed the NIR band is necessary for the surface nature resource classification and achieve the improvement from 91.21% to 91.72% of OA and from 90.59% to 91.23% of F1-score.

But the results of our models have not peaked and the building, flower nursery and road have low accuracy. As our future work, we will try more models to classify the surface nature resources and solve the problem that some classes have low accuracy.

5. Acknowledgements

The work was supported in part by the Open Fund of Key Laboratory of Urban Land Resources Monitoring and Simulation, Ministry of Natural Resources (Grant No. KF-2018-03-063 Grant No. KF-2019-04-069, and Grant No. KF-2019-04-074,); Science Research Program of Natural Resources Department of Sichuan Province (Grant No. KJ-2020-3); Opening Foundation of Guangxi Key Laboratory for Spatial Information and Geomatics, Guangxi, China (Grant No. 17-259-16-14 and Grant No. 19-050-11-06), the Key Technologies Research and Development Program of Sichuan Province (Grant No. 2020YFSY0041); and the Open Fund of State Key Laboratory of Water Resources and Hydropower Engineering Science (Grant No. 2014SWG04, and Grant No.2018SWG02).

References

[1] Lamine. S, Petropoulos. G. P, Singh. S. K, Szabó. S, Bachari. N. E. I, Srivastava. P. K, and Suman. S, "Quantifying land use/land cover spatio-temporal landscape pattern dynamics from Hyperion using SVMs classifier and FRAGSTATS", Geocarto international, vol 33, No. 8, pp. 862-878, 2018.

[2] Bin Zhang, Cunpeng Wang, Yonglin Shen, and Yueyan Liu, "Fully connected conditional random fields for high-resolution remote sensing land use/land cover classification with convolutional neural networks", Remote Sensing, Vol 10, No. 12, pp. 1889, 2018.

[3] Cuicui Ji, Xiaosong Li, Huaidong Wei, and Sike Li, "Comparison of Different Multispectral Sensors for Photosynthetic and Non-Photosynthetic Vegetation Fraction Retrieval", Remote Sensing, Vol 12, No. 1, pp. 115, 2020.

[4] Yilu Gong, Xueming Li, Xueping Cong, and He Liu, "Research on the Complexity of Forms and Structures of Urban Green Spaces Based on Fractal Models", Complexity, pp. 2020, 2020.

[5] Jindong Wang, Yiqiang Chen, Shuji Hao, Xiaohui Peng, and Lisha Hu, "Deep learning for sensor-based activity recognition: A survey," Pattern Recognition Letters, vol. 119, pp. 3-11, 2019.

[6] Tao Liu, and Abd-Elrahman. A, "An object-based image analysis method for enhancing classification of land covers using fully convolutional networks and multi-view images of small unmanned aerial system", Remote Sensing, Vol 10, No. 3, pp. 457, 2018.

[7] Xuning Liu, Yong Zhou, Jiaqi Zhao, Rui Yao, Bing Liu, Ding Ma, and Yi Zheng, "Multiobjective ResNet pruning by means of EMOAs for remote sensing scene classification", Neurocomputing, Vol 381, pp. 298-305, 2020.

[8] Zemin Han, Yuanyong Dian, Hao Xia, Jingjing Zhou, Yongfeng Jian, Chonghuai Yao, Xiong Wang, and Yuan Li, "Comparing Fully Deep Convolutional Neural Networks for Land Cover Classification with High-Spatial-Resolution Gaofen-2 Images", ISPRS International Journal of Geo-Information, Vol 9, No. 8, pp. 478, 2020.

H3DNN: 3D DEEP LEARNING BASED DETECTION OF COVID-19 VIRUS USING LUNGS COMPUTED TOMOGRAPHY

ABDULLAH AMAN KHAN[1], SIDRA SHAFIQ[2], RAJESH KUMAR[1], JAY KUMAR[1], AMIN UL HAQ[1]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, China
[2]Department of Computer Science, The Women University Multan, Punjab, Pakistan
E-MAIL: abdkhan@std.uestc.edu.cn, sid.siduuu@gmail.com, rajakumarlohano@gmail.com, jay@std.uestc.edu.cn, khan.amin50@yahoo.com

Abstract:

With the rapid spread of the novel COVID-19 virus, there is an increasing demand for screening COVID-19 patients. Typical methods for screening coronavirus patients have a large false detection rate. An effective and reliable screening method for detecting coronavirus is required. For this reason, some other reliable methods such as Computed Tomography (CT) imaging is employed to detect coronavirus accurately. In this paper, we present a 3D-Deep learning based method that automatically screens coronavirus patients using 3D volumetric CT image data. Our proposed system assists medical practitioners to effectively screen out COVID-19 patients. We performed extensive experiments on two datasets i.e., CC-19 and COVID-CT using various state-of-the-art 3D Deep learning based methods including 3D ResNets, C3D, 3D DenseNets, I3D, and LRCN. The results of the experiments show the competitive effectiveness of our proposed approach.

Keywords:

COVID-19; Coronavirus; 3D deep learning; Deep learning; Artificial intelligence

1. Introduction

Due to the rapid spread of the novel COVID-19 virus, the Artificial Intelligence (AI) research community explored many ideas for diagnosing lung infection by analyzing Computed Tomography (CT) imaging [1-3]. The initial reason behind this attention towards chest CT imaging was the lack of nucleic acid-based CoVID-19 detection kits. After observing the high false-negative rate of nucleic acid test, clinical practitioners started to prefer screening of COVID-19 patients via chest CT imaging [4]. Specifically, for early-stage detection, CT imaging offers a glass-like clarity to highlight lesions of the lung. However, according to the radiologists, clinical screening of COVID-19 is still unsatisfactory [5-7]. Therefore, automated screening with the help of AI can assist clinical practitioners to improve screening accuracy.

Over the past few months, many deep learning based screening approaches have been proposed to detect infected lesions from 2D CT imaging [7-9]. Unfortunately, they either demand a high percentage of annotated areas of lesions or lack of interpretability. Generally, the standard pioneer input for the classifiers is either patch-based or lesion-based. However, the 3D volume of CT imaging is still not well explored. The exploitation of 3D volume is under consideration to improve the screening accuracy. Compared with classic 2D CT images, the generated 3D volume of CT usually contains hundreds of slices which are more difficult to analyze even for the clinical practitioners.

Previously proposed deep learning models, such as [5][6][10], cannot be directly applied for 3D imaging. Therefore, there exists a need to design an automated model to detect lung infection caused by COVID-19 from 3D chest CT imaging.

In this paper, we propose a Hybrid 3D Deep Neural Network model (H3DNN) to classify chest CT imaging. The model is developed by ensembling the Inflated inception (I3D) and 3D ResNet 50 to build a common architecture for capturing the Spatio-temporal dimension including the inception block. Unlike previous approaches, H3DNN can semantically generate deep 3D samples with permutation-invariance to improve network accuracy. The main contributions of our work are given as follows:

- We propose an automated 3D deep learning model (H3DNN) to classify 3D chest CT imaging to screen out infected patients.
- Our approach can easily diagnose the early stage of COVID-19 patients by considering Spatio-temporal features and constructing 3D filters.
- We conducted extensive experiments on two available datasets. The results of the experiments boldly show the significance of H3DNN.

978-1-7281-4242-5/19/$31.00 ©2019 IEEE

2. Proposed Method

In this section, we elaborate on our proposed 3D deep learning network. 3D deep learning based models efficiently make use of Spatio-temporal information that utilizes 3D convolutions and other relevant blocks. Such networks have achieved higher performance in many Artificial Intelligence (AI) applications. AI based automation has already proven itself in other domains [11-13].

The proposed network can be considered as a hybrid of a single stream I3D [14] and a 3D ResNet 50 [15] network model. 3D deep learning models bootstraps 3D convolution filters based on 2D convolutions. I3D utilizes a receptive field for an artificial neural network (ANN). However, when a temporal dimension is included it requires finding an optimal receptive field.

Inflated inception: I3D utilizes the inception block as shown in Figure 1. The main motivation of this module is to allow the network to grow wider instead of deeper. The I3D network model is represented by the block C in Figure 2. The I3D network starts with a 3D convolution layer with a stride of 2 followed by a MaxPool layer having a stride of (1,2,2). Further, two convolution layers are followed by a MaxPool layer having a stride of (1,2,2). The resultant of this Maxpool layer is then fed to two inception blocks. Further, another MaxPool layer is followed by five more inception blocks. The resultant is then forwarded to a MaxPool with a stride of 2 attached to two more inception blocks. Finally, an average pooling is carried out and the resultant is passed on to a convolution layer followed by a fully connected layer.

3D ResNet: A unitary ResNet block consists of two convolution layers fed to a batch normalization (BN) and ReLU [16] layers. A bypass connects the top block to the layer before ReLu. The ResNet 3D block extracts more valuable features as compared to 2D. The ResNet architecture is represented by block A in Figure 2. The first convolution layer with a stride of 64 is followed by six consecutive convolution layers. Further, eight more convolution layers are added with a stride of 128. The resultant is forwarded to a block of twelve convolution layers with a stride of 256 followed by a block of six convolution layers. Finally, average pooling is carried out followed by a 400d fully connected layer.

Hybrid model (H3DNN): I3D and 3D ResNet 50 are capable of extracting prominent features from Spatio-temporal data. We feed both the network models with a sequence of CT scan images. In our case, we feed a series of 60 and 35 CT scan images. The reason for choosing these numbers is that some of the patients' CT scan images in the datasets contain a minimal of 60 and 35 CT scan slices/images. The input CT scan sequence was first resized $224 \times 224 \times 3$ to match the input profile of the targeted 3D feature extraction network. The slices are fed to I3D and 3D ResNet block separately. Each feature extraction extracts Spatio-temporal features. Further, each 3D block i.e. Block A and Block C in Figure 2 are used to train fully connected layers [17]. The probability output of the fully connected layers is then added and the resultant fed to a Softmax layer [18], which, finally classifies the suspect as positive or negative.

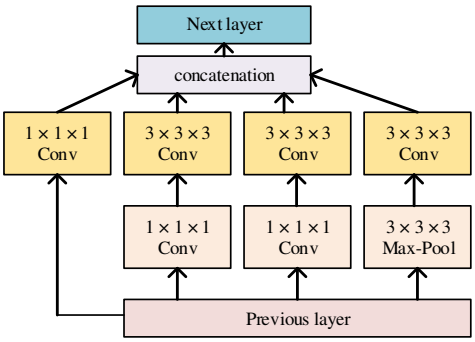


Fig. 1 Inception block of I3D network. The parameters from the previous layer are the input to this block where the next layer represents the output of the inception block.

3. Experiments and results

We performed extensive experiments on two publically available CC-19 [8] and COVID-CT [19] datasets. First, we provide some details about the CC-19 and COVID-CT datasets. We used these datasets as they contain the required series of CT scan images for 3D analysis.

3.1. Datasets

CC-19 dataset: contains about 34,000 CT scan images for 89 subjects. Out of 89, 68 subjects are confirmed COVID-19 patients. CC-19 dataset contains a huge amount of data. The data was recorded on a day to day basis for every subject. CC-19 dataset was collected from various hospitals in Sichuan, China.

COVID-CT: This dataset contains CT scan images for 349 scans from 216 patients and 463 CT scans from non-covid subjects. Both of these datasets were confirmed by professional radiologists.

3.2. Experiment setup

All the experiments were performed on an Intel Xeon 40 core processor equipped with Ubuntu 20.04.1 LTS operating system, 128 GB RAM, hard drive 6 Gbps data bandwidth, and 08 Tesla K80 graphic processing units

(GPU). All the experiments were carried out using Keras with a TensorFlow backend.

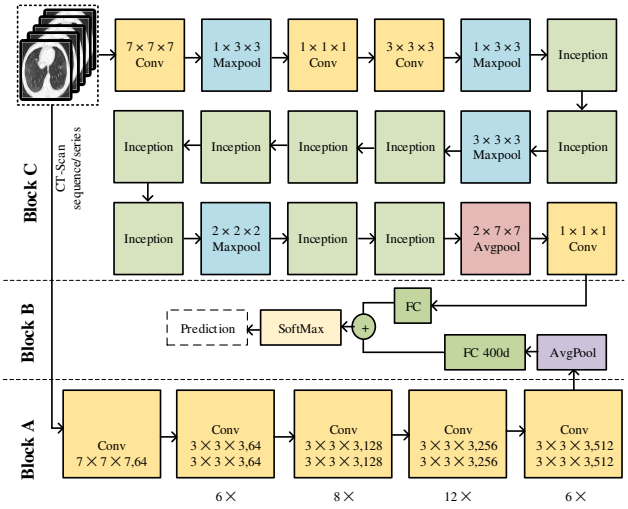


Fig. 2 Our proposed hybrid network model.

We trained I3D and 3D ResNet 50 from scratch. Further, the individual weights of the best-trained models were saved. 3D networks are hard to train as they require more computational resources, the batch size for training was kept 2. These models were trained using Adams' optimizer with a learning rate of 10^{-5} and a decay rate of 10^{-6}. We use these smaller values as we trained the network from scratch. Moreover, we used an early stopping machoism with patience of 5 with 1000 epochs at maximum. For 3D ResNet 50, the regularization factor was set to 2.5×10^{-2}.

3.3. Results

We performed comprehensive experiments to validate the proposed model. The results of the experiments are shown in Table 1. The accuracy is computed as $Acc = (TP + TN)/(TP + TN + FP + FN)$. Where, TP, TN, FP, and FN are the true positive, true negative, false positive, and false negative respectively.

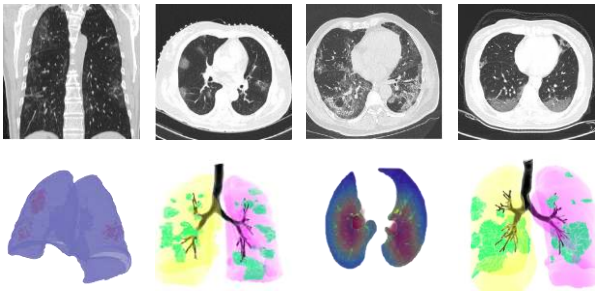


Fig.3 3D visualization with various ways of our proposed model. The top left image shows the XZ plane of the 3D volume.

From Table 1, it can be seen that our proposed model H3DNN showed superior performance. Figure 3 shows some 3D visualization of the 3D CT scans from these datasets. We believe, the reason behind the superiority of our model is that it combines the goodness of both I3D and 3D Resnet 50 deep learning models.

Table 1. Comparison of our proposed technique with state-of-the-art methods. Moreover, S and Acc. Represents the number of CT slices and accuracy respectively. C-CT represents the COVID-CT dataset.

Method	Size	CC-19		C-CT	
		S	Acc.	S	Acc
C3D [20]	150×150	60	0.76	35	0.81
LRCN [21]	150×150	60	0.73	35	0.76
3D Conv [20]	100×100	60	0.76	35	0.75
DenseResNet3D [15]	112x112	60	0.76	35	0.74
DenseNet 3D [15]	112×112	60	0.76	35	0.75
I3D [14]	224×224	60	0.80	35	0.81
R2Plus1D [22]	171×128	60	0.76	35	0.75
3D ResNet 18 [23]	224×224	60	0.76	35	0.77
3D ResNet 34 [23]	224×224	60	0.76	35	0.79
3D ResNet 50 [23]	224×224	60	0.83	35	0.82
3D ResNet 101 [23]	224×224	60	0.78	35	0.77
3D ResNet 151 [23]	224×224	60	0.80	35	0.80
H3DNN	224×224	60	0.85	35	0.84

4. Conclusion

In this paper, we proposed a hybrid 3D deep learning model (H3DNN). H3DNN makes use of I3D and 3D Resnet 50 to screen out COVID-19 patients. The proposed model automatically and effectively detects the COVID-19 patients at a low cost in terms of annotations of CT images. We conducted comprehensive experiments using two available datasets. The results of the experiments reveal the superiority of our proposed method. In the future, we plan to design a full multimedia system for doctors that can effectively segment and point out the infections caused by the COVID-19 virus.

References

[1] D. P. Fan et al., "Inf-Net: Automatic COVID-19 Lung Infection Segmentation from CT Images," IEEE Trans. Med. Imaging, 2020, doi: 10.1109/TMI.2020.2996645.

[2] R. Kumar et al., "An Integration of Blockchain and AI for Secure Data Sharing and Detection of CT images for the Hospitals," Comput. Med. Imaging Graph.,

2020.
[3] X. Ouyang et al., “Dual-Sampling Attention Network for Diagnosis of COVID-19 from Community Acquired Pneumonia,” IEEE Trans. Med. Imaging, 2020, doi: 10.1109/TMI.2020.2995508.
[4] V. M. Corman et al., “Detection of 2019 novel coronavirus (2019-nCoV) by real-time RT-PCR,” Eurosurveillance, 2020, doi: 10.2807/1560-7917.ES.2020.25.3.2000045.
[5] Y. Oh, S. Park, and J. C. Ye, “Deep Learning COVID-19 Features on CXR Using Limited Training Data Sets,” IEEE Trans. Med. Imaging, 2020, doi: 10.1109/TMI.2020.2993291.
[6] S. Roy et al., “Deep Learning for Classification and Localization of COVID-19 Markers in Point-of-Care Lung Ultrasound,” IEEE Trans. Med. Imaging, 2020, doi: 10.1109/TMI.2020.2994459.
[7] X. Ouyang et al., “Dual-Sampling Attention Network for Diagnosis of COVID-19 From Community Acquired Pneumonia,” IEEE Trans. Med. Imaging, vol. 39, no. 8, pp. 2595–2605, 2020.
[8] R. Kumar et al., “Blockchain-Federated-Learning and Deep Learning Models for COVID-19 detection using CT Imaging,” arXiv. 2020.
[9] G. Wang et al., “A Noise-Robust Framework for Automatic Segmentation of COVID-19 Pneumonia Lesions from CT Images,” IEEE Trans. Med. Imaging, 2020, doi: 10.1109/TMI.2020.3000314.
[10] L. Zhou et al., “A Rapid, Accurate and Machine-Agnostic Segmentation and Quantification Method for CT-Based COVID-19 Diagnosis,” IEEE Trans. Med. Imaging, 2020, doi: 10.1109/TMI.2020.3001810.
[11] A. A. Khan, J. Shao, W. Ali, and S. Tumrani, “Content-Aware Summarization of Broadcast Sports Videos: An Audio–Visual Feature Extraction Approach,” Neural Process. Lett., 2020, doi: 10.1007/s11063-020-10200-3.
[12] A. A. Khan, H. Lin, S. Tumrani, Z. Wang, and J. Shao, “Detection and localization of scorebox in long duration broadcast sports videos,” 2020, doi: 10.1117/12.2575834.
[13] S. Tumrani, Z. Deng, A. A. Khan, and W. Ali, “PEVR: Pose Estimation for Vehicle Re-Identification,” in Asia-Pacific Web (APWeb) and Web-Age Information Management (WAIM) Joint International Conference on Web and Big Data, 2019, pp. 69–78.
[14] J. Carreira and A. Zisserman, “Quo Vadis, action recognition? A new model and the kinetics dataset,” 2017, doi: 10.1109/CVPR.2017.502.
[15] Z. Qiu, T. Yao, and T. Mei, “Learning Spatio-Temporal Representation with Pseudo-3D Residual Networks,” 2017, doi: 10.1109/ICCV.2017.590.
[16] Y. Li and Y. Yuan, “Convergence analysis of two-layer neural networks with RELU activation,” 2017.
[17] X. Glorot and Y. Bengio, “Understanding the difficulty of training deep feedforward neural networks,” 2010.
[18] B. D. Ripley, Pattern recognition and neural networks. 2014.
[19] J. Zhao, X. He, X. Yang, Y. Zhang, S. Zhang, and P. Xie, “COVID-CT-Dataset: A CT image dataset about COVID-19,” arXiv. 2020.
[20] D. Tran, L. Bourdev, R. Fergus, L. Torresani, and M. Paluri, “Learning spatiotemporal features with 3D convolutional networks,” 2015, doi: 10.1109/ICCV.2015.510.
[21] J. Donahue et al., “Long-Term Recurrent Convolutional Networks for Visual Recognition and Description,” IEEE Trans. Pattern Anal. Mach. Intell., 2017, doi: 10.1109/TPAMI.2016.2599174.
[22] D. Tran, H. Wang, L. Torresani, J. Ray, Y. Lecun, and M. Paluri, “A Closer Look at Spatiotemporal Convolutions for Action Recognition,” 2018, doi: 10.1109/CVPR.2018.00675.
[23] K. Hara, H. Kataoka, and Y. Satoh, “Learning spatio-Temporal features with 3D residual networks for action recognition,” 2017, doi: 10.1109/ICCVW.2017.373.

THE APPLICATION RESEARCH ON MILITARY INTERNET OF THINGS

LI XIANLI[1], PAN WEI[2], AN JIANYONG[1], WAN PING[1]

[1]Military Logistics Department, Army Logistics University of PLA, Chongqing, China
[2]32366 troops of PLA, Beijing, China
E-MAIL: lixianli1818@163.com, plapw@sina.com, 2874143819@qq.com, 1035380280@qq.com

Abstract:

Internet of things is a research hotspot in recent years, and the development of Military Internet of things is still in its infancy. This paper mainly discusses the concept of military Internet of things, studies key technologies of military Internet of things, and analyses the application of military Internet of things in the field of battlefield perception, weapons and equipment management, logistics support, military training and so on, and some key technical problems are proposed. AS the development of military Internet of things, the application will be constantly renewing, so, it is of great significance to the research of military Internet of things.

Keywords:

Military Internet of things (MIOT); Radio Frequency Identification; Wireless Sensor Network; Military Application

1. Introduction

Military Internet of Things (MIOT) is an application of Internet of things in the military areas. Military Internet of things takes "realizing information interaction between the real physical world and the virtual computer world" as the fundamental concept, breaks through the original mode of computer network, and represents the future of computer technology and communication technology. Therefore, it is called the third wave of information technology revolution by many countries, and it is another important milestone of information industry after computer, Internet and mobile communication network. The development of Internet of things technology is pregnant with a new opportunity for the further development of military reform, and has broad application prospects in the military field.

2. Overview of Military Internet of Things

Military Internet of things is the specific application of Internet of things technology in the military field. Based on Internet of things technology, it can build a huge network system covering the core military application such as battlefield awareness, operation command, equipment management, logistics support, etc. The carrier of "seamless link from sensor to transmitter" is exactly the military Internet of things technology, Military Internet of things promotes the new military reform. Based on Internet of things, MIOT extends the application to the information battlefield space, and extends the user end to any element of the battlefield. Through the perception, transmission, processing and application of information, it has created a different intelligent battlefield.

2.1. Concept of Military Internet of Things

Military Internet of things is a fusion system of military physical system and digital information system, it is an intelligent information network that combines military facilities, combat equipment, weapons and fighters with military network, so as to realize the interconnection between things, people and things, and people to people. Conceptually, each element in the network (such as weapons and equipment, logistics materials, commanders, individual soldiers, etc.) is a network node. All elements are integrated into the military information network through Internet of things technology, and military action is supported by military information.

Military Internet of things is a comprehensive and deep integration of physical system and digital information system in various military fields through intelligent connection in the network. Using Internet of things technology to obtain the status characteristics of military entities in military activities, such as personnel, weapons, equipment and battlefield environment, etc. According to the standard communication protocol, through the military sensor and communication network system, the information interaction and communication between personnel, equipment, weapons and battlefield environment are realized, and all kinds of information obtained by information perception nodes are intelligently processed, controlled, managed and applied, so as to realize the interconnection between any time, any place and any object in military fields.

2.2. Architecture of Military Internet of Things

Military Internet of things is a three-layer architecture which is composed of perception layer, network layer and application layer. The perception layer of MIOT is composed of sensors, electronic tags, intelligent terminals, etc. it uses intelligent equipment to collect information, identify objects, and transmit information to network layer. The network layer of military Internet of things transmits and processes the information obtained from sensing layer through wired and wireless network technology. Based on military information network, a fast, convenient, stable and reliable sensor network is formed under the strong support of cloud computing platform. The application layer of military Internet of things has very comprehensive and detailed military application solutions, such as battlefield awareness, weapon equipment management, medical assistance and military logistics. Based on military Internet of things, all weapons and equipment, commanders, combat forces, logistics support forces and command centers can be integrated into an interconnected, highly networked and information-based whole. The architecture of military Internet of things is shown in Figure1 below.

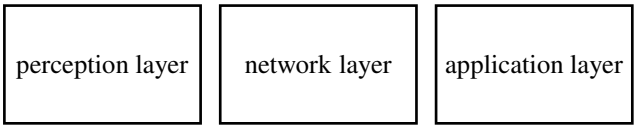


Fig.1 The architecture of MIOT

2.3. Key Technologies of Military Internet of Things

Internet of things is a huge network that combines various information devices, such as radio frequency identification (RFID), infrared sensors, global positioning system (GPS), laser scanners, etc. all objects are connected with the network to realize intelligent identification, positioning, tracking, monitoring and management. It embodies the three-layer architecture of Internet of things: perception layer, network layer and application layer.

Military Internet of things also follows such a three-layer architecture model, which embodies three important characteristics of military Internet of things: thorough perception, extensive interconnection and intelligent application. The three important features determine key technology composition of each layer of MIOT, perception layer emphasizes the accuracy, timeliness and purposefulness of perception, recognition and positioning, network layer includes horizontal and vertical information exchange, application layer mainly include big data, cloud computing, artificial intelligence and other intelligent analysis technologies. Figure 2 illustrates key technologies of perception layer, key technologies of network layer, and key technologies of application layer.

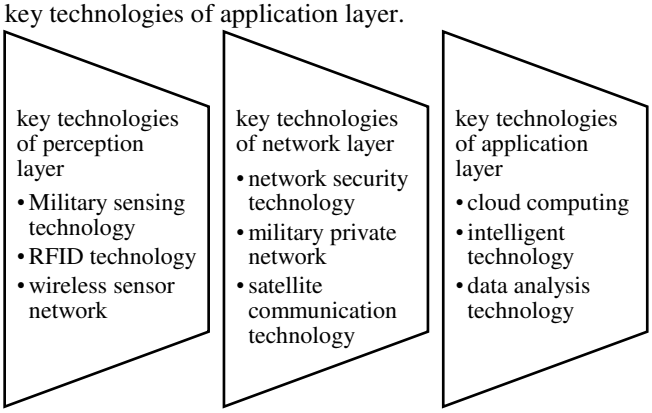


Fig.2 The key technologies of MIOT

3. Typical Application of Military Internet of Things

The typical application of military Internet of things mainly include real-time battlefield awareness, intelligent control of weapons and equipment, joint precision support, etc. through the seamless connection from sensors to transmitters in the objective physical world in the military field, MIOT realizes multi-dimensional perception, multi-domain interconnection, full controllability, and whole network for war, which improves the accuracy and automation of combat attack under the condition of informatization, future battlefield will be more transparent, more intelligent in operational command, more accurate in logistics support and more secure in battlefield monitoring. Figure 3 illustrates some applications of MIOT.

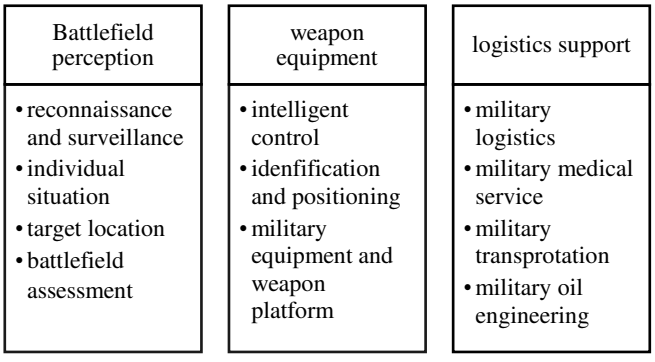


Fig.3 The application of MIOT

3.1. Real-time perception of battlefield environment

On the battlefield, commanders need to know the supply conditions of troops, weapons, equipment and

military materials timely and accurately. The sensor network will collect the corresponding information, send the data to the command post through the sink node, and then transmit the data to the headquarters through the network, and finally integrate the data from various battlefields to form a complete situation map. In the war, the sensor network which is laid manually or spread by aircraft or guns can observe the enemy closely in a more concealed way, and can also provide accurate target positioning information for the fire control and guidance system.

Information is the core resource in modern war. Whoever has the right to control information will have the initiative in the whole war. However, the only way to gain the "right to control information" is to get information quickly in modern wars. The initiative of the battlefield largely depends on who can discover the enemy first, and the acquisition of "first opportunity" depends on the perception network. In the future, with the help of the Internet of things technology, we will form a perception battlefield with various sensors that are pre-deployed in the form of temporary delivery, so as to accurately sense all kinds of operational information of both sides of the enemy and our side, and form an omni-directional, full spectrum and full time domain reconnaissance, monitoring and early-warning system, realize the connection with the command and control system, and ensure the integration of reconnaissance, monitoring and attack.

3.2. Intelligent control of weapon equipment

Using military Internet of things to establish equipment management network of joint battlefield equipment, weapon platform and military carrier platform, it can dynamically perceive, statistics and analysis the information of vehicle, weapon and platform, and can realize the control of equipment positioning, distribution, movement state, service life and cycle, maintenance information, and so on, so as to realize the intelligent management of weapons and equipment in the macro monitoring of military Internet of things.

Weapons and equipment are the material basis of the army's combat effectiveness and the basic conditions for the army to perform its functions. Management of weapons and equipment is an important part of the regular management of the army. Using MIOT to build the intelligent monitoring system and management system of weapons and equipment can improve the level of precision, informatization and remote management of weapons and equipment, meet the requirements of flexible scheduling and safely using of weapons and equipment, and realize multi-level, efficient and flexible communication and management.

3.3. Informatization construction of logistics support

The military Internet of things is based on the Internet of things technology, which is widely used in the informatization construction of military logistics fields, and can effectively improve combat training ability and joint logistics support efficiency of the army. The application of military Internet of things in logistics field mainly includes military logistics, military medical service, military transportation, military oil engineering, etc.

(1) Application in military logistics. Military logistics is the dynamic management of military materials. Through the processing of logistics information, it makes the collection, packaging, transportation, storage and sorting of military materials accurate, efficient, safe and controllable. Based on the Internet of things technology, it improves the dynamic adaptability of the supply support system, and automatically obtains the information of equipment and materials in storage, in operation and in use. Through the intelligent perception and automatic transmission means of MIOT, it can realize real-time monitoring of all links in the process of military logistics, timely grasp the status of military logistics activities, and respond in real time, so as to integrate all links more closely, realize the integration of internal information resources, control the inventory quantity, reduce the imbalance between supply and demand, improve service quality, and form an end-to-end intelligent supply chain of military logistics.

(2) Application in military medical service. Internet of things technology has great potential application in the military medical and health field, which provides an effective technical support for the realization of medical information digitization, diagnosis intelligence and drug material management visualization of military medical and health system. The Internet of things and its related intelligent technologies provide broad prospects for military mobile medical and nursing, drug equipment support, environmental monitoring and three prevention inspection, medical rescue, military health monitoring and military telemedicine. In the military hospital information system, the electronic medical record (EMR) based on the Internet of things technology can finish the complete record of whole process of treatment in hospital through the collection, storage, transmission, processing and utilization of the information of medical personnel, so as to realize the informatization of the whole medical process.

(3) Application in military transportation. The object recognition, global positioning, object tracking and other technologies of MIOT provide strong technical support for intelligent management in the field of military transportation. They are widely used in military railway, waterway and air

transportation scheduling system, dynamic tracking of military transport vehicles, information parking and military vehicle anti-counterfeiting. Among them, based on Beidou II satellite positioning technology, geographic information system (GIS), display technology and information transmission technology, the dynamic tracking system of army transport vehicle can grasp the status and resource information of transport vehicles, and can locate, track, command, and dispatch the vehicle in real time, and it can dynamically achieve accurate geographical coordinates and accurate delivery time, and take accurate route to provide accurate quantity of equipment and materials to the troops in demand, so, it can greatly improve the efficiency of command and dispatch. Through the combination of Internet of vehicles, information collection, information exchange protocol, intelligent monitoring and management technology, it can query the status information of transportation vehicles, transportation environment, transportation support force in real time, and it can effectively provide decision-making information. Through the combination with material identification technology, it can realize the visualization of transportation materials, improve the accuracy of materials supply, and greatly promote the informatization construction of military logistics support.

With the continuous development of the research and application of MIOT, the informatization level of our army's logistics support will be improved day by day. We will gradually realize the accurate perception of the support situation, the precise delivery of material support, the independent intelligence of logistics equipment, and the efficient command and control. In the future war, we can truly realize the real-time perception of every corner of the battlefield and accurately support all units of the battlefield, and undertake the historical mission to win victory in information age.

4. Technical Challenges

The military application based on Internet of things is in full swing, and all countries want to seize the top position in this technical field. Many key technologies have not been combined with practical application, but its development is very rapid. In order to apply the Internet of things technology in all aspects of the military field, we need to constantly combine the breakthrough in the technical field with the practical application. We can foresee that in the near future, the Internet of things technology will lead to new military innovation. In the process of MIOT development, the main challenges are as follows.

4.1. Information Security Obstacle

Compared with the traditional network, the sensor nodes in military Internet of things are usually deployed in the area where the physical attack can reach, the complexity of military Internet of things, the universality of distribution, the diversity of forms and the limitation of node resources make the military Internet of things more vulnerable to intrusion than the general system, and it faces more serious security problems. When all devices are intelligent and networked, the concept of boundary will be further weakened. How to ensure the security of military Internet of things is an urgent obstacle to be broken.

4.2. Standardization issues

At present, there are various sensor identification, and there are more than 250 kinds of RFID alone. It will be a long and arduous process to unify all kinds of protocol standards. The establishment of “China Internet of things standards joint working group” in 2020 is of great significance for accelerating the standardization of military Internet of things and deepening the application of the military Internet of things.

4.3. Data Processing problem

The basis of military Internet of things is a huge sensing network, which aggregates the acquired data and finally provides the basis for the decision-making system. All of these need the support of data fusion technology, data mining technology, cloud computing, data compression technology, artificial intelligence theory and intelligent signal processing technology. How to deal with massive data is an urgent problem.

5. Conclusion

Although the application and development prospect of military Internet of things is very broad, we must also be soberly aware that there are still many factors and hidden dangers restricting the development of military Internet of things. As a new concept, the military Internet of things is still in the stage of exploration in various applications.

References

[1] Hao Huihui. Application of Internet of things technology in Intelligent Logistics[J]. Information and computer (theoretical edition), No.7, pp.13-15, 2020.

[2] Li Zhenyu. Application of Internet of things in hospital network information management[J], Network security technology and application, No.11, pp.144-146, 2020.
[3] Zheng Jinguang. Application analysis of Internet of things based on 5G technology[J]. Application of integrated circuit, No.10, pp.58-59, 2020.
[4] Wu Hequan. Overview of the application and challenges of the Internet of things[J]. Journal of Chongqing University of Posts and Telecommunications, Vol.22, No. 5, pp. 526-531, 2010.
[5] Lu Minhui, Zhang guomin. Internet of things technology and its application in military field[J]. Journal of Naval Engineering University, Vol.8, No.4, pp. 43-48, 2011.
[6] Song Hang, Li Jiancheng, Zhang Chunhua, Wu Jianfei. Key technologies of military Internet of things[J]. National Defense Science and Technology, Vol.36, No.6, pp. 24-34, 2015.

AN APPLICATION OF SVD++ METHOD IN COLLABORATIVE FILTERING

SHENG JIANG[1], JIANPING LI[1], WANG ZHOU[2]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, P. R. China
2School of Computer and Software Engineering, Xihua University, Chengdu 610039, P.R. China
E-MAIL: js20121002@163.com, jpli2222@uestc.edu.cn, dean_uestc@163.com

Abstract:

Collaborative filtering algorithms have important applications in the implementation of recommendation systems. Collaborative filtering generally focuses on the user's evaluation scores for commodity items, and these evaluation data imply some specific relevance. Therefore, this type of collaborative filtering Model research has attracted widespread attention. SVD is currently one of the most classic and practical collaborative filtering algorithm models. It can deal with the problem of data sparseness in the recommendation system and derive different types of SVD models on this basis, but its recommendation results It has never been significantly improved. In response to such problems, this article proposes a new variant of the SVD++ algorithm that incorporates a special timing mechanism for dynamic adjustment, and uses the average absolute error, root mean square error and standard average absolute error for the recommended results. After evaluation, we got better results than the current classic SVD++ model.

Keywords:

Collaborative Filtering; Singular Value Decomposition; Recommendation System; Time Series Data

1. Introduction

Collaborative filtering is a common technology used to reduce information overload and has become the main tool of personalized recommendation systems. The nearest neighbor collaborative filtering algorithm is currently one of the most successful recommendation techniques[1]. However, with the expansion of the recommendation system[2], the extreme sparseness of user rating data has led to the reduction of the recommendation quality of the algorithm. In order to solve the problem of data sparsity, an SVD matrix factorization method proposed by Kalman et al. was introduced in 1996 to be used in the recommendation system[3]. However, this Traditional-SVD[4-5] on large-scale data, SVD decomposition will reduce the program speed. Moreover, the SVD decomposition method has a single feature and the effect is not obvious; the FunkSVD[6] algorithm published in the Simon Funk blog in 2006, avoids the sparse problem of the matrix, is decomposed into two matrices, and has achieved good results in practical applications; in FunkSVD After the algorithm became popular, many improved FunkSVD algorithms appeared. Among them, BiasSVD adds the feature of bias items on the basis of FunkSVD, which will perform better than FunkSVD in some scenes; SVD++[7] is a further improvement of BiasSVD[8], introducing implicit feedback and user attribute information, which is equivalent to introducing additional Information sources, which can reflect user preferences from the side, and can solve the cold start problem caused by fewer explicit scoring behaviors;

This paper will consider the time series model to mine the trend of time series data characteristics, and combines it with the traditional SVD++ algorithm model to also improve the effectiveness of the recommendation results[9], and the effect of the model is better than the current classic SVD++ model algorithm.

2. SVD singular matrix factorization model

2.1. Singular Value Decomposition

The form of SVD decomposition is the multiplication of 3 matrices, and the intermediate matrix is a singular value matrix. If you want to use SVD decomposition, there is a premise that the matrix is required to be dense, that is, the elements in the matrix must be non-empty, otherwise SVD decomposition cannot be used. Obviously, SVD cannot be used for our task, so the general approach is to fill the matrix with the mean or other statistical methods first, and then use SVD decomposition. In the dimensionality reduction theory, SVD can also be used directly for recommendation. We can use User -Item score matrix A is decomposed by SVD, and dimensionality is reduced at the same time by selecting some

of the larger singular values, that is to say, matrix A is decomposed into:

$$A_{m\times n} \approx U_{m\times K}\sum_{m\times K}V^T{}_{k\times n} \quad (1)$$

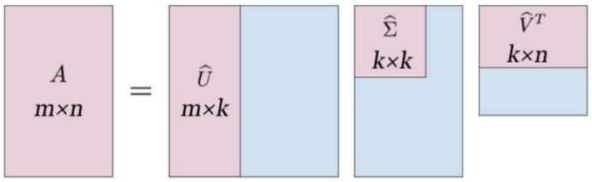


Fig.1 Decomposition diagram of matrix A

Usually we are a great approximation of SVD, because for the recommendation system, it is not when extreme accuracy is required, we are more pursuing efficiency and maximization of profit. This form can greatly reduce the amount of calculation and is more in line with actual needs. Through singular value decomposition, if we want to predict the rating $a_{ij}$of the i-th user for the i-th item, we only need to calculate $u_i\Sigma u^T{}_j$. In this way, we can get a predicted score for all the unrated positions in the score table, and recommend to the user by finding the items with the highest scores.

2.2. FunkSVD model

The FunkSVD method published by Simon Funk on his blog is a matrix factorization method called latent factor model (LFM) by Yehuda Koren. Its starting point is that since it is time-consuming to SVD decompose a matrix into three matrices, and at the same time face the problem of sparseness, then we try to avoid the problem of sparseness and decompose into only two matrices at the same time, that is, we now expect our matrix R is decomposed like this:

$$R_{m\times n}=P_{m\times k}\times Q_{k\times n} \quad (2)$$

This simplified matrix decomposition is no longer decomposed into three matrices, but into two low-rank user and item matrices. In fact, both users and items are mapped into a k-dimensional space. This k-dimensional space corresponds to There are k hidden factors. We believe that users' ratings of items are mainly affected by these hidden factors, so these hidden factors represent the common features of a part of the user and the item, which appear as attribute characteristics on the item and preference characteristics on the user. It's just that these hidden factors do not have practical meaning, nor do they necessarily have very good interpretability. There is no definite label name for each dimension, so they are called "hidden factors". So how FunkSVD decomposes the sparse matrix R into reasonable P and Q. Machine learning algorithms are used here. In fact, the idea of linear regression is applied. Our goal is to let users have scores and score residuals obtained by matrix products. The difference is as small as possible, so the mean square error is used as the loss function to find the final P and Q. That is, the user feature matrix and item feature matrix Q learned through User-Item rating information, and the reconstructed low-dimensional matrix is used to predict the user's rating of the item.

Suppose that a user u rating for item i is r_{ui}, the implicit feature vector of the corresponding user u that is projected into the k-dimensional space through matrix decomposition is p_u, and the implicit feature vector of the corresponding item i is q_i, in the two vectors The elements of represents respectively the degree of conformity of the user u and the item i to the hidden factors, there are positive and negative. The dot product of two implicit eigenvectors can be used to approximate the original value before matrix decomposition, which expresses the user u overall interest in items, expressed as:

$$\hat{r}_{ui}=q^T{}_i p_u \quad (3)$$

Regarding r_{ui} as the real score and r_{ui} as the predicted score, for all samples with existing scores, the objective function can be obtained:

$$\min_{q^*,p^*}\sum_{(u,i)}\left(r_{ui}-q^T{}_i p_u\right)^2+\lambda\left(||p_u||^2+||q_i||^2\right) \quad (4)$$

Among them, κ is a sample set of user and item pairs that have been rated, and λ is a regularization coefficient, which is a hyperparameter.

$$\frac{\partial J}{\partial p_u}=-2\left(r_{ui}-q^T{}_i p_u\right)q_i+2\lambda p_u \quad (5)$$

$$\frac{\partial J}{\partial q_i}=-2\left(r_{ui}-q^T{}_i p_u\right)p_u+2\lambda q_i \quad (6)$$

In the iteration of the gradient descent method, the iteration formula of p_u、q_i :

$$p_u=p_u+\alpha[(r_{ui}-q^T{}_i p_u)q_i-\lambda p_u] \quad (7)$$

$$q_i=q_i+\alpha[(r_{ui}-q^T{}_i p_u)p_u-\lambda q_i] \quad (8)$$

Through iteration, we can finally get p and q, which could then be used for recommendation. Although the idea of FunkSVD algorithm is very simple, the effect is very good in practical application, which really proves the simple way.

2.3. BiasSVD model

Take the Netflix Prize recommendation competition[10] data set as an example, Yehuda Koren only uses the bias part to compare The scoring error is reduced by 32%, and the addition of the personalized part can reduce it by 42%, which means that only 10% is the role of the personalized part, which fully illustrates the importance of the bias part, and the remaining 58% The error Yehuda Koren will call the

unexplainable part of the model, including factors such as data noise. The bias part is mainly composed of three sub-parts, namely:

1) The global average of all scoring records in the training set, $\boldsymbol{\mu}$ represents the overall scoring of the training data. For a fixed data set, it is a constant.

2) User bias $\boldsymbol{b_u}$, a factor independent of item characteristics, represents the scoring habits of a particular user. For example, critical users are more demanding on their own scores and tend to give low scores; while optimistic users have more conservative scores and overall scores are higher.

3) The item bias $\boldsymbol{b_i}$, which is independent of the user's interest, represents the scoring situation of a particular item. Take movies as an example. Good movies get a high overall score, while bad movies get a low score. This feature is captured by item bias.

So, the predicted score plus the bias part is:

$$\hat{\boldsymbol{r}}_{\boldsymbol{ui}}=\boldsymbol{u}+\boldsymbol{b_u}+\boldsymbol{b_i}+\boldsymbol{q}^{\boldsymbol{T}}{}_{\boldsymbol{i}}\boldsymbol{p_u} \quad (9)$$

The objective function $\boldsymbol{J(p,q)}$ is:

$$\min_{p^*,q^*,b^*} \sum_{(u,i)\in\kappa}\left(\boldsymbol{r_{ui}}-\boldsymbol{u}-\boldsymbol{b_u}-\boldsymbol{b_i}-\boldsymbol{q}^{\boldsymbol{T}}{}_{\boldsymbol{i}}\boldsymbol{p_u}\right)+\boldsymbol{\lambda}\left(||\boldsymbol{p_u}||^2+||\boldsymbol{q_i}||^2+\boldsymbol{b_u^2}+\boldsymbol{b_i^2}\right) \quad (10)$$

This optimization goal can also be solved by the gradient descent method. The difference with FunkSVD is that at this time we have two more bias terms $\boldsymbol{b_u}$ and $\boldsymbol{b_i}$, $\boldsymbol{p_u}$and $\boldsymbol{p_i}$ the iteration formula of and is similar to FunkSVD, except that the gradient derivative of each step is slightly different. And $\boldsymbol{b_u}$ and $\boldsymbol{b_i}$ generally can be initially set to a 0 vector, and then participate in the iteration.

$$\boldsymbol{b_u}=\boldsymbol{b_u}+\boldsymbol{\alpha}\left(\boldsymbol{r_{ui}}-\boldsymbol{u}-\boldsymbol{b_u}-\boldsymbol{b_i}-\boldsymbol{q}^{\boldsymbol{T}}{}_{\boldsymbol{i}}\boldsymbol{p_u}-\boldsymbol{\lambda b_u}\right) \quad (11)$$

$$\boldsymbol{b_i}=\boldsymbol{b_i}+\boldsymbol{\alpha}\left(\boldsymbol{r_{ui}}-\boldsymbol{u}-\boldsymbol{b_u}-\boldsymbol{b_i}-\boldsymbol{q}^{\boldsymbol{T}}{}_{\boldsymbol{i}}\boldsymbol{p_u}-\boldsymbol{\lambda b_i}\right) \quad (12)$$

Through iteration, we can finally get $\boldsymbol{p}$ and $\boldsymbol{q}$, which can then be used for recommendation. BiasSVD adds some additional considerations, so it will perform better than FunkSVD in some scenes.

2.4. SVD++ model

SVD++ is a further improvement of BiasSVD. It introduces implicit feedback and user attribute information, which is equivalent to the introduction of additional information sources, which can reflect user preferences from the side, and can solve the cold caused by less explicit scoring behaviors. Startup problem. Let me first talk about how to add implicit feedback. The method is: In addition to assuming that the items in the rating matrix have a hidden factor vector, the set of items for which the user has acted also has a hidden factor vector, with the same dimensions. The hidden factor vectors of items manipulated by the user are added together to express the user's interests and preferences.

Similarly, after user attributes such as sociological statistical information are all converted into 0-1 features, it is also assumed that there is a hidden factor vector of the same dimension for each feature, and the hidden factor vectors corresponding to all attributes of a user are added. Which also represents some of his preferences.

Combining the two, in the objective function of SVD++, only the recommendation score prediction part needs to be slightly modified. The original user vector part adds an implicit feedback vector and a user attribute vector:

$$\hat{\boldsymbol{r}}_{\boldsymbol{ui}}=\boldsymbol{u}+\boldsymbol{b_u}+\boldsymbol{b_i}+\boldsymbol{q_i^T}\left(\boldsymbol{p_u}+|\boldsymbol{N_u}|^{-0.5}+\sum_{\boldsymbol{j}\in\boldsymbol{N_{(u)}}}||\boldsymbol{x_j}||^2+\sum_{\boldsymbol{\alpha}\in\boldsymbol{A_{(u)}}}||\boldsymbol{y_a}||^2\right) \quad (13)$$

The objective function is：

$$\boldsymbol{min}\sum_{\boldsymbol{r_{ui}}\in\boldsymbol{R_{train}}}(\boldsymbol{r_{ui}}-\hat{\boldsymbol{r}}_{\boldsymbol{ui}})^2+\boldsymbol{\lambda}\left(||\boldsymbol{p_i}||^2+||\boldsymbol{q_i}||^2+\boldsymbol{b_u^2}+\boldsymbol{b_i^2}+\sum_{\boldsymbol{j}\in\boldsymbol{N_{(u)}}}||\boldsymbol{x_j}||^2+\sum_{\boldsymbol{a}\in\boldsymbol{A_{(u)}}}||\boldsymbol{y_a}||^2\right) \quad (14)$$

Among them, $\boldsymbol{N_{(u)}}$ is $\boldsymbol{u}$ the collection of items produced by user u, and $|\boldsymbol{N_u}|^{-0.5}$ is a normalization factor, which can bring a good effect on the normalization of the sum; it is hidden, for The personal preference bias of product j (equivalent to every product that produces behavior has a preference $\boldsymbol{x_j}$) is a parameter we need to learn. And $\boldsymbol{x_j}$ is a vector, the number of dimensions is equal to the number of hidden factor dimensions, and each component represents the degree of preference for a certain hidden factor component of the commodity, that is to say, summing $\boldsymbol{x_j}$ is actually the hidden factor corresponding to all the commodities that produce behaviors. The factor component values are respectively summed, and the final summed vector is equivalent to the user's preference for these hidden factors; $\boldsymbol{A_{(u)}}$ is the attribute set of user u, $\boldsymbol{y_a}$ is similar to $\boldsymbol{x_j}$, that is, each attribute All correspond to a hidden factor vector, which is also a parameter to be learned.

The overall optimization learning algorithm of SVD++ remains unchanged, but the parameters to be learned have two more vectors: $\boldsymbol{x}$ and $\boldsymbol{y}$, one is the item vector of implicit feedback, and the other is the vector of user attributes.

3. SVD++ model-based Time Series

This section will introduce in detail the recommended algorithm based on time series model and matrix factorization proposed in this article, describe the algorithm design idea, analyze and derive the objective function. The core of the traditional probability matrix factorization model is to learn the eigenvectors of users and items, and predict the score of unknown items based on the eigenvectors. However,

in this scenario, the user's behavior in each time period is known, and it is necessary to predict the user's behavior in the future time period, and the user's behavior is often regular in time. Using these rules can dig out the user's potential interest preferences. Drift situation.

fig.2 shows the timing information of a user's commodity purchase behavior. The data shows that the user's interest in the four products M1~M4 in the four time periods has the following law: interest in the two products M1 and M4 shows a decreasing trend, and interest in the two products M2 and M3 shows an increasing trend. Therefore, in the future time T5, recommending the two products M2 and M2 for users is more in line with user preferences. In the actual data set, the amount of data is usually much larger than the example in fig. 2, and the actual data set is usually highly sparse. This article is difficult to analyze the trend of data changes through direct observation, so the method of data prediction using raw data is not possible. Combining the characteristics of the implicit behavior of time series data and the good performance of probabilistic matrix decomposition in processing large-scale data sets, this paper uses a method of combining time series models and matrix decomposition to improve recommendation efficiency. First, confirm that you have the correct template for your paper size. This template has been tailored for output on the US-letter paper size. If you are using A4-sized paper, please close this template and download the file for A4 paper format called "CPS_A4_format".

Given a time series T= $\{t_1, t_2, t_3, t_4, \ldots t_L\}$, L represents the length of the time series. The method in this paper mainly includes two steps:

Probabilistic matrix decomposition is performed on the music listening matrix of a certain time period t_L to obtain the user feature matrix U_{t_L} and item feature matrix V_{t_L} of the current time period. The dimension of each feature vector is K, so that user U and the item.

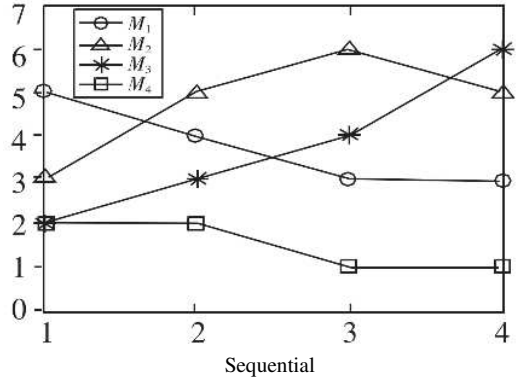


Fig. 2 Time sequence diagram of the number of user purchases

The eigenvector of V satisfies a spherical Gaussian prior with zero mean:

$$p\left(U_{t_L}\middle|\sigma_{U_{t_L}}^2\right) = \prod_{i=1}^{N} N\left(U_{it_L}\middle|0, \sigma_{U_{t_L}}^2, I\right) \quad (15)$$

$$p\left(U_{t_L}\middle|\sigma_{V_{t_L}}^2\right) = \prod_{j=1}^{N} N\left(U_{jt_L}\middle|0, \sigma_{V_{t_L}}^2, I\right) \quad (16)$$

After obtaining the feature vector of each time period, combine the SVD model to obtain the time series model of each feature vector in the L time period, and predict the feature vector of the user i in the L+1 time period as U_{iL+1}, L+1 time the eigenvector of item j of the segment is V_{jL+1}. The original eigenvector sequence is fitted by a differential, and the SVD model parameters are fitted according to the time series data of the eigenvectors, and then the parameters are substituted into the SVD model to predict the next period value.

$$U_{iL+1} = \nabla_{i1}U_L + \nabla_{i2}U_{L-1} + \cdots + \nabla_{ix}U_{L-x} + \beta_{i1}U_L - \delta_{i1}\beta_{iL-1} - \cdots \delta_{iy}\beta_{iL-y}; \quad (17)$$

$$V_{jL+1} = \nabla_{j1}V_L + \nabla_{j2}V_{L-1} + \cdots + \nabla_{jx}V_{L-x} + \beta_{j1}V_L - \delta_{j1}\beta_{jL-1} - \cdots \delta_{jy}\beta_{jL-y}; \quad (18)$$

After predicting the user feature matrix U_{L+1} and item feature matrix V_{L+1} in the L+1 time period, the original function of matrix decomposition can be used to calculate the predicted purchase number matrix R_{L+1} in the L+1 time period.

4. Evaluation index

4.1. Evaluation Metric

The root means square error (Root Mean Square Error, RMSE) is the square root of the ratio of the sum of squares of deviations between the observations and the true value to the number of observations m. It is used to measure the deviation between the observed value and the true value.

$$RMSE(X,h) = \sqrt{\frac{1}{m}\sum_{i=1}^{m}(h(x^{(i)}) - y^{(i)})^2} \quad (19)$$

Mean Absolute Error (MAE) is the average value of absolute error, which can better reflect the actual situation of predicted value error.

$$MAE(X,h) = \frac{1}{m}\sum_{i=1}^{m}\left|h\left(x^{(i)}\right) - y^{(i)}\right)| \quad (20)$$

Standard Deviation (SD) is the arithmetic square root of variance, which is used to measure the degree of dispersion of a set of numbers.

$$\text{SD}=\sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - u)^2}\, u \quad (21)$$

where u represents the average value

$$u = \frac{1}{N}(x_1 + \cdots ... + x_N). \quad (22)$$

4.2. Algorithm recommendation effect comparison

The experiment first compares the recommendation effect of the algorithm in this paper and the comparison algorithm under the same conditions[11]. In the experiment, set the feature vector dimension k=5,10,20. For time series of different lengths, experiments are performed on commodity 1, commodity 2, and commodity 3. The other parameters of the algorithm are set to the corresponding values when each algorithm is optimal.

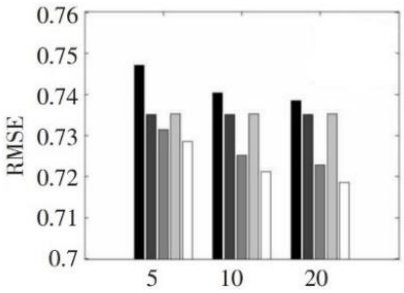


Fig.3 RMSE result of commodity 1

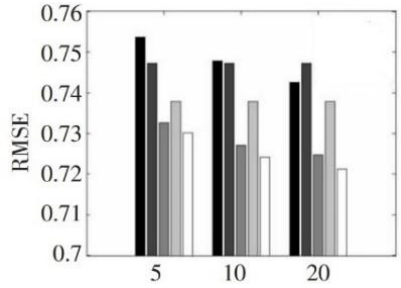


Fig.4 RMSE result of commodity 2

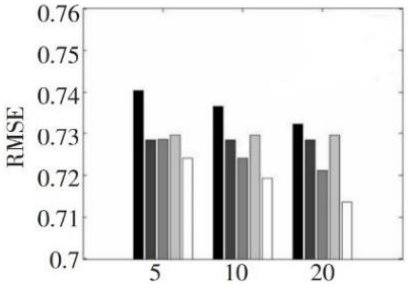


Fig.5 RMSE result of commodity 3

As the length of the time series increases, the data volume of the data set becomes larger, and the recommendation effect of the algorithm also improves with the increase of the data volume[11]. The experimental results show that the SVD++ method combined with time information could greatly improve than the basic SVD method. Compared with the traditional methods, the method in this paper has better results in the recommendation accuracy and the quality of the recommendation list, which fully illustrates that the time factor is effective in solving the problem. The problem of user interest shift is valid and reasonable. The method in this paper only needs relatively easy-to-obtain user behavior time information, so the actual application scenarios of the algorithm are more extensive, and it gives new ideas for the expansion of the matrix decomposition model of large-scale data[12].

5. Conclusions

This paper uses the time series information of user shopping behavior to propose a recommendation algorithm combining time series model and SVD singular matrix decomposition. First, it analyzes and summarizes the existing recommendation algorithm based on matrix factorization, and then proposes an improved method for the shortcomings of the traditional SVD method. Compared with tags, location information, etc., user behavior time information is easier to obtain, and probabilistic matrix decomposition has good recommendation accuracy for high-dimensional matrices and matrix sparsity issues, so this article combines the advantages of timing and SVD++ to improve recommendation efficiency. Experiments on real shopping datasets show that the method in this paper has better recommendation effects than existing algorithms, has better performance on RMSE and MAE numerical indicators, and can effectively control the time complexity of the algorithm, so it is more suitable for large Personalized recommendation task in data environment.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, the project of Science and Technology Department of Chongqing Municipality, Chengdu Chengdian Network Technology Co., Ltd., Chengdu Civil-military Integration Project Management Co., Ltd., and Sichuan Yin Ten Gu Technology Co., Ltd.

References

[1] P. Cremonesi, A. Tripodi, and R. Turrin, "Cross-Domain Recommender Systems," in 2011 IEEE 11th International Conference on Data Mining Workshops,

Dec. 2011, pp. 496–503, doi: 10.1109/ICDMW.2011.57.
[2] D. Kalman, “A Singularly Valuable Decomposition: The SVD of a Matrix,” Coll. Math. J., vol. 27, no. 1, p. 2, 1996, doi: 10.2307/2687269.
[3] P. Resnick and H. R. Varian, “Recommender systems,” Commun. ACM, vol. 40, no. 3, pp. 56–58, Mar. 1997, doi: 10.1145/245108.245121.
[4] H. C. Andrews and C. L. Patterson, “Singular Value Decomposition (SVD) Image Coding,” IEEE Trans. Commun., vol. 24, no. 4, pp. 425–432, 1976, doi: 10.1109/TCOM.1976.1093309.
[5] A. Höcker and V. Kartvelishvili, “SVD approach to data unfolding,” Nucl. Instruments Methods Phys. Res. Sect. A Accel. Spectrometers, Detect. Assoc. Equip., vol. 372, no. 3, pp. 469–481, 1996, doi: 10.1016/0168-9002(95)01478-0.
[6] R. Salakhutdinov and A. Mnih, “Probabilistic matrix factorization,” Adv. Neural Inf. Process. Syst. 20 - Proc. 2007 Conf., pp. 1–8, 2009.
[7] Y. Koren, “Factor in the neighbors: Scalable and accurate collaborative filtering,” ACM Trans. Knowl. Discov. Data, vol. 4, no. 1, pp. 1–24, 2010, doi: 10.1145/1644873.1644874.
[8] M. Hayakawa, “MF Techniques,” Earthq. Predict. with Radio Tech., pp. 199–207, 2015, doi: 10.1002/9781118770368.ch6.
[9] C. Bakir, “Collaborative filtering with temporal dynamics with using singular value decomposition,” Teh. Vjesn., vol. 25, no. 1, pp. 130–135, 2018, doi: 10.17559/TV-20160708140839.
[10] X. Tan and P. Pan, “A Contextual Item-Based Collaborative Filtering Technology,” Intell. Inf. Manag., vol. 04, no. 03, pp. 85–88, 2012, doi: 10.4236/iim.2012.43013.
[11] G. Linden, B. Smith, and J. York, “Amazon.com recommendations: item-to-item collaborative filtering,” IEEE Internet Comput., vol. 7, no. 1, pp. 76–80, Jan. 2003, doi: 10.1109/MIC.2003.1167344.
[12] M. Grbovic and H. Cheng, “Real-time personalization using embeddings for search ranking at Airbnb,” Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Min., pp. 311–320, 2018, doi: 10.1145/3219819.3219885.

ORCA OPTIMIZATION ALGORITHM: A NEW META-HEURISTIC TOOL FOR COMPLEX OPTIMIZATION PROBLEMS

NOORBAKHSH AMIRI GOLILARZ[1], HUI GAO[1], ABDOLJALIL ADDEH[2], SAEID PIRASTEH[3]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[2]Faculty of Electrical and Computer Engineering, Babol Noshirvani University of Technology, Babol, Iran
[3]Faculty of Geosciences & Environmental Engineering, Southwest Jiaotong University, Chengdu 611756, China
E-MAIL: noorbakhsh.amiri@std.uestc.edu.cn, huigao@uestc.edu.cn, jalil_addeh@yahoo.com, sapirasteh@swjtu.edu.cn

Abstract:

In this paper, a new meta-heuristic algorithm called Orca Optimization Algorithm (OOA) is proposed for complex and nonlinear optimization problems, especially practical engineering problems. This developed method is based on unique wave-washing orcas hunting technique. In the OOA, different random candidates (orcas) implement the cunning tactic of regularly hunting in packs and building waves to wash seals off drifting piece of ice. Application of the proposed algorithm on some benchmark functions including Schaffer, Griewank, Ackley, and Rosenbrock proved its excellent capability in comparison with other similar algorithms such as Genetic Algorithm (GA), Flower Pollination Algorithm (FPA), Harris Hawk Optimization (HHO) algorithm, and Imperialist Competitive Algorithm (ICA). Moreover, the performance of the proposed optimization algorithm applied on real engineering problems. In this experiment, OOA applied for online parameter estimation of photovoltaic modules equivalent circuit and optimal design of brushless direct current (BLDC) motor. The numerical analysis and obtained simulation results of the experiments showed the excellent performance of OOA.

Keywords:

Orca; Wave-washing technique; Local minima; Convergence speed; Engineering optimization problems

1. Introduction

Optimization is the process by which the best solution (according to a set of criteria) is selected from a set of possible solutions to a particular problem. Today, optimization problems are used in all quantitative disciplines such as computer science, engineering, operations research, economics, medicine, data analysis, and more. Over the centuries, the development of methods for generating solutions and problem solving has been an important area of research in mathematics, and their importance has multiplied over the past few years. Many optimization problems in the engineering sciences are more complex and difficult than can be solved by conventional optimization methods such as mathematical programming methods and the like.

Due to the importance of the issue, in recent years, various nature-based optimization algorithms in particular bee algorithm (BA) [1], particle swarm algorithm (PSO) [2], imperialist competitive algorithm (ICA) [3], cuckoo optimization algorithm (COA) [4], Harris hawk optimization (HHO) algorithm [5], Flower Pollination Algorithm (FPA) [6], and genetic algorithm (GA) [7] have been proposed to solve optimization problems. These meta-heuristic optimization algorithms do not require a derivative of the objective function; therefore, can be applied on any optimization problem. These algorithms have been widely used to solve various practical problems [8- 14]. Most of the developed algorithms, such as PSO algorithms, do not have good global search capability and easily get caught in the trap of local minima. Newer algorithms such as the bat algorithm and the COA are also very complex and have a high computational volume that is not suitable for solving problems in which it is very important to find the optimal solution in a short time. For example, in the COA, the data is clustered in each iteration of the algorithm. The clustering technique used in this optimization algorithm is the K-Means clustering method, which does not perform well and easily gets caught in the trap of local minimums [15]. In GA, many operators such as elitism, roulette wheel, mutation, crossover, and selection require high-volume computations in each iteration of the algorithm. This computation burden greatly reduces the speed of the GA. In ICA, there are various operators such as attracting colonies, revolution, and roulette wheel, which leads to increasing the volume of calculations.

By studying the previous studies, it can be justified that in designing population-based optimization algorithms, two points including exploration and exploitation should be considered so that the algorithm has good accuracy and

convergence speed. In the population-based optimization algorithms, the exploration indicates the algorithm's capacity to inspect the different unknown areas in the solution interval to catch the global optimum point. While, the exploitation indicates to the algorithm's capacity to employ the knowledge of the prior good solutions to discover and catch the optimum solution. Given these issues and the importance of the issue, a new optimization method has been proposed in this study, which is inspired by the Orca's hunting technique. More information regarding the new developed optimization algorithm is given in the remaining sections.

2. Proposed OOA Algorithm

2.1. Orcas in nature

Certain types of Antarctic orcas employ the cunning strategy of frequently hunting in a group and building powerful waves to wash seals off floating piece of ice. This unique performance was first observed in late 1970s, but at the time it was recognized as a one-time behavior. From then until today, marine researchers have reported several similar observations [16]. The orcas repeat this process in different directions until the prey (seal) falls from the ice into the sea. This unique tactic and strategy are shown in Figure 1. More detail regarding orcas' wave-washing techniques can be found in [16].

Fig.1 A group of orcas utilizing waves for knocking seals off the ice floe in nature [17]

2.2. OOA

In Orca algorithm, orcas wash the ice floe in different directions with different energies. The energy of each orca determines its ability to wash the ice floe and get closer to the seal (X_s). The orca can wash the ice floe and reduce its area. In this process, orcas are in the determined area by radius R at random direction. The orcas that are located farther away from ice floe have higher velocity when reach to ice floe and wash it with higher energy. On the other hand, the orcas that are near to ice floe, have lower energy when they hit the ice floe. Figure 2 shows this concept.

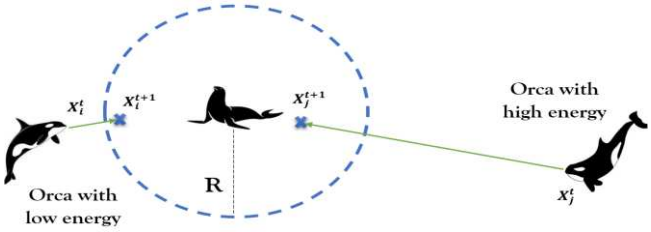


Fig.2 Ice floe washing by orcas

In this figure, the farther orca can hit the ice floe with more energy and get closer to the seal. To model this behavior, we used the energy of orcas to determine the new position of orcas. The energy of each orca can be calculated using the following equations in the proposed algorithm:

$$e_i = F_i - F_s \tag{1}$$

Where, F_i and F_s indicate the fitness of X_i and X_s respectively. Then, we sort the energy vector $[e]_{N\times 1}\}$, and determine the orca with highest and lowest energy. According to sorted energy vector, we compute the normalized value of energies using the following equation:

$$E_i = \frac{e_i - e_{min}}{e_{max} - e_{min}} \tag{2}$$

The orca moves toward the ice floe and lie somewhere between the two circles (the highlighted area) as shown by Figure 3. The first circle's radius is R and the second circle's radius is (R-d):

$$d_i = E_i \times R \tag{3}$$

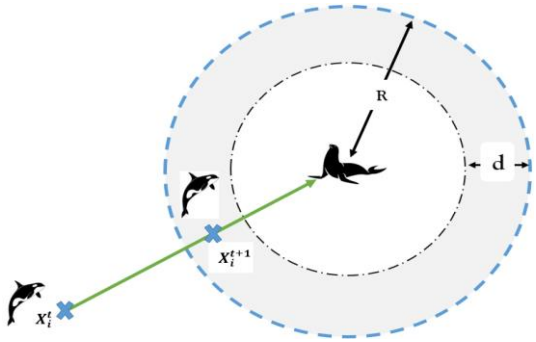


Fig.3 Wave washing and reducing the area of ice floe in the OOA

At each iteration, P percent of orca population will be eliminated and generate in the search space randomly. This process allows the algorithm to escape from local minima. Algorithm 1 shows the Pseudo code of the proposed algorithm

Alg.1 Pseudo code of the proposed OOA algorithm

Generate initial population of orcas (N+1) in search space randomly
Determine the initial radius ($R = R_0$) of ice floe
Calculate the fitness of each orca and sort them
while (stopping condition is not met) **do**

- Assign the best answer as the Seal (X_s)
- Compute the normalized energy of each orca (E_i) by Eq. (1) and (2)
- Move the orcas toward the Seal and ice floe using according to their energy in the area determined by Eq. (3)
- Remove the worst orcas (P%) and generate them randomly for the next iteration

endwhile

3. Result

3.1. Performance on benchmark functions

For evaluating the performance of OOA, four widely used benchmark functions including generalized Schaffer (f_1), Griewank (f_2), Rosenbrock (f_3), and Ackley (f_4) are utilized. Their mathematical expressions are stated by Eq. (4) to (7). In table 1, initial range of unknown variables, their optimal value and global optimum answer (minimum of function) are listed. In this table, D indicates the dimension of function or number of unknown variables that should be find by OOA.

$$f_1(\vec{x}) = \frac{\sin^2\left(\sum_{i=1}^{D} x_i^2\right) - 0.5}{\left(1 + 0.001\left(\sum_{i=1}^{D} x_i^2\right)\right)^2} + 0.50 \qquad (4)$$

$$f_2(\vec{x}) = \frac{1}{4000}\left(\sum_{i=1}^{D}(x_i - 100)^2\right) - \left(\prod_{i=1}^{D} \cos\left(\frac{x_i - 100}{\sqrt{i}}\right)\right) + 1.0 \qquad (5)$$

$$f_3(\vec{x}) = \sum_{i=1}^{D-1} 100(x_{i+1} - x_i^2)^2 + (x_i - 1)^2 \qquad (6)$$

$$f_4(\vec{x}) = 20 + e - 20\exp\left(-0.2\sqrt{\frac{1}{D}\sum_{i=1}^{D} x_i^2}\right) - \exp\left(\frac{1}{D}\sum_{i=1}^{D}\cos(2\pi x_i)\right) \qquad (7)$$

Table 1 Benchmark functions

Function	Range	Optimal answer	Minimum point
$f_1(\vec{x})$	$[-100, 100]^D$	$[0, 0, \dots, 0]$	0.0
$f_2(\vec{x})$	$[-600, 600]^D$	$[100, \dots, 100]$	0.0
$f_3(\vec{x})$	$[-50, 50]^D$	$[1, 1, \dots, 1]$	0.0
$f_4(\vec{x})$	$[-32.768, 32.768]^D$	$[0, 0, \dots, 0]$	0.0

The obtained results using proposed method and other similar optimization algorithms such as GA, FPA, PSO algorithm, HHO algorithm, and ICA are listed in Tables 2 to 5 and Figure 4. In the experiments, the number of initial populations for all algorithms are set to 30 and the algorithm is continued for convergence point with 20 iterations without any change. All the listed values in tables are the average of 20 unrelated and separate implementation of different optimization algorithms on benchmark functions. The best performance is obtained by OOA

Table 2 Performance of different algorithms on generalized Schaffer function ($f_1(\vec{x})$) by three and six unknown variables

algorithms	D= 3			D= 6		
	Mean	SD	Iterations	Mean	SD	Iterations
GA	$7.23\ E-6$	$2.85\ E-5$	179	$7.23\ E-6$	$2.85\ E-5$	251
PSO	$6.19\ E-11$	$3.93\ E-8$	162	$6.19\ E-11$	$3.93\ E-8$	236
HHO	$8.52\ E-15$	$5.83\ E-12$	81	$8.52\ E-15$	$5.83\ E-12$	92
ICA	$4.76\ E-13$	$8.21\ E-9$	104	$4.76\ E-13$	$8.21\ E-9$	153
FPA	$7.54\ E-11$	$7.22\ E-9$	125	$7.54\ E-11$	$7.22\ E-9$	168
OOA	**0**	**0**	**59**	$\mathbf{2.54\ E-17}$	$\mathbf{1.03\ E-14}$	**73**

Table 3 Performance of different algorithms on Griewank function ($f_2(\vec{x})$) by 30 and 60 unknown variables

algorithms	D= 30			D= 60		
	Mean	SD	Iterations	Mean	SD	Iterations
GA	$3.22\ E-8$	$6.42\ E-8$	197	$7.23\ E-6$	$2.85\ E-5$	219
PSO	$6.53\ E-12$	$3.91\ E-12$	165	$6.19\ E-11$	$3.93\ E-8$	201
HHO	$7.03\ E-16$	$5.83\ E-17$	85	$8.52\ E-15$	$5.83\ E-12$	132
ICA	$3.96\ E-14$	$4.81\ E-15$	115	$4.76\ E-13$	$8.21\ E-9$	149

FPA	$7.29\,E-12$	$2.67\,E-13$	99	$7.54\,E-11$	$7.22\,E-9$	141
OOA	$\mathbf{5.67\,E-19}$	$\mathbf{1.93\,E-20}$	**72**	$\mathbf{2.81\,E-13}$	$\mathbf{5.28\,E-14}$	**92**

Table 4 Performance of different algorithms on Rosenbrock function ($f_3(\vec{x})$) by two and three unknown variables

algorithms	D= 2			D= 3		
	Mean	SD	Iterations	Mean	SD	Iterations
GA	$1.61\,E-3$	$2.21\,E-3$	156	$5.14\,E-2$	$6.10\,E-3$	192
PSO	$5.72\,E-3$	$2.83\,E-4$	142	$9.94\,E-2$	$9.21\,E-3$	174
HHO	$2.08\,E-4$	$8.67\,E-5$	83	$3.25\,E-4$	$5.94\,E-3$	102
ICA	$4.53\,E-3$	$2.67\,E-4$	95	$7.29\,E-3$	$3.77\,E-3$	129
FPA	$7.44\,E-3$	$2.67\,E-4$	90	$7.29\,E-2$	$4.21\,E-3$	133
OOA	$\mathbf{6.18\,E-5}$	$\mathbf{2.01\,E-5}$	**61**	$\mathbf{9.84\,E-4}$	$\mathbf{5.77\,E-5}$	**83**

Table 5 Performance of different algorithms on Ackley function ($f_4(\vec{x})$) by 30 and 60 unknown variables

algorithms	D= 30			D= 60		
	Mean	SD	Iterations	Mean	SD	Iterations
GA	$7.61\,E-3$	$6.21\,E-11$	132	$5.14\,E-2$	$4.31\,E-9$	171
PSO	$3.72\,E-3$	$7.11\,E-12$	126	$5.14\,E-2$	$6.45\,E-10$	154
HHO	$6.94\,E-3$	$1.76\,E-15$	89	$5.14\,E-2$	$1.67\,E-14$	125
ICA	$9.55\,E-3$	$5.97\,E-14$	94	$5.14\,E-2$	$6.29\,E-12$	137
FPA	$6.09\,E-3$	$9.72\,E-13$	103	$5.14\,E-2$	$9.37\,E-12$	139
OOA	$\mathbf{3.49\,E-18}$	$\mathbf{5.32\,E-17}$	**73**	$\mathbf{7.15\,E-16}$	$\mathbf{5.77\,E-15}$	**96**

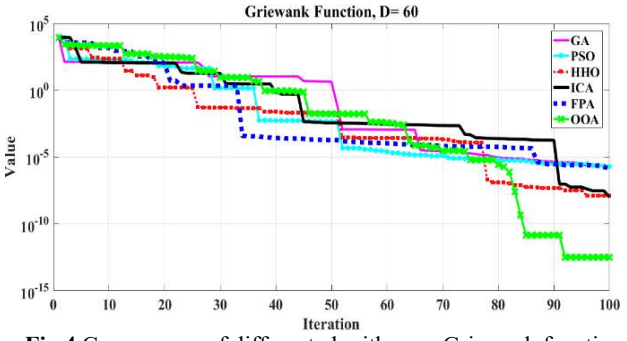


Fig.4 Convegence of different algoithm on Griewank function, D=60

3.2. Application on PV circuit parameter estimation

The solar photovoltaic (PV) modeling is one of the most important issues in this filed and erroneous current-voltage (I-V) curve formation introduces less efficiency. The PV equivalent circuits can be used in different experimental applications and control schemes. The most commonly used approach for PV modules modelling is two-diode model (TDM). In the equivalent circuit, Figure 5, parameters are not constant and will be changed by changing environmental conditions. The I-V formulation of TDM is stated by Eq. (8) to (11) [18].

$$I_{\mathrm{D1}} = \mathrm{I_{O1}}\left[\exp\left(\frac{V_D}{\alpha_1 V_T}\right)-1\right] \quad (8)$$

$$I_{\mathrm{D2}} = \mathrm{I_{O2}}\left[\exp\left(\frac{V_D}{\alpha_2 V_T}\right)-1\right] \quad (9)$$

$$I_{pv} = I_{pv,n} - I_{D1} - I_{D2} - \frac{V_{pv}+I_{pv}R_s}{R_p} \quad (10)$$

$$I_{PV} = I_{pv.n} - I_{o1}\left[exp\left(\frac{V_{PV}+I_{PV}R_s}{\alpha_1 V_T}\right)-1\right] - I_{o2}\left[exp\left(\frac{V_{PV}+I_{PV}R_s}{\alpha_2 V_T}\right)-1\right] - \left(\frac{V_{PV}+I_{PV}R_s}{R_P}\right) \quad (11)$$

where $V_T = \frac{KT}{q}$, $K = 1.381e-23$ is Boltzmann constant and $q = 1.602e-19$ is the charge of an electron. In addition, T shows the temperature of environemnt in Kelvin [18].

In this section, OOA is used for estimation of PV equivalent circuit parameters. The proposed method updates these parameters considering environment condition including irradiation (G) and Temperature (T). For modelling a PV array, its equivalent circuit parameters, i.e., reverse saturation currents I_{o1} and I_{o2}, series resistance R_s, shunt resistance R_p, factor of diode ideality or emission coefficient α_1 and α_2, and PV module current $I_{pv,n}$, must be updated so that the I-V curve of the resultant circuit closely emulates the measured I-V curve of the real PV array. In the proposed method, Mean Absolute Error (MAE) of model current (I_{est}) and experimentally measured currents (I_m) is used as fitness function of optimization algorithm.

$$MAE = \frac{1}{M}\sum_{k=1}^{k=m}(|I_m(k) - I_{est}(k)|) \quad (12)$$

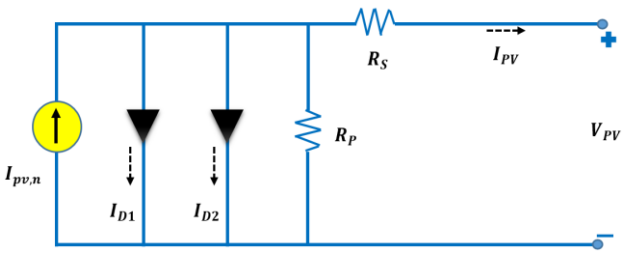


Fig. 5 TDM equivalent electrical circuit

The G and T are the input of OOA and I_{o1}, $I_{o2}, \alpha_1, \alpha_2$, $R_s, R_p, I_{ph,n}$ are the output. The OOA and other optimization algorithms are applied on SPR-415E-WHT-D Sun Power series modules. The obtained results are listed in Table 6, and it can be seen that the proposed OOA had the best performance. In addition, Figure 6 shows the performance of OOA

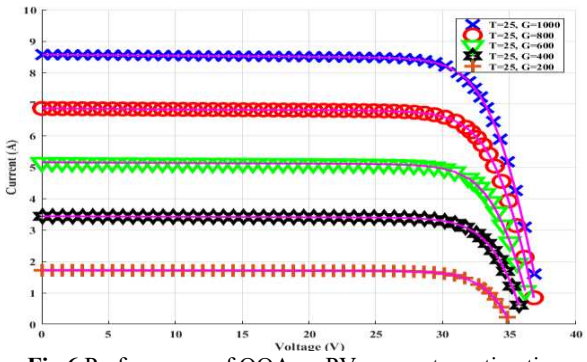


Fig.6 Performance of OOA on PV parameter estimation

Table 6 Performance of different algorithms on PV parameter estimation problem

algorithms	MAE
GA	$5.74\ E-3$
PSO	$4.93\ E-3$
HHO	$9.05\ E-4$
ICA	$3.66\ E-3$
FPA	$7.18\ E-3$
OOA	$\mathbf{2.83\ E-4}$

3.3. Application on motor design

The permanent magnet brushless direct current (BLDC) motors are progressively being used for medical and industrial applications. These motors have excellent features such as small size and weight that makes them suitable choice for medical applications, large power to volume ratio, good efficiency, low tremor, excellent dynamic response, good reliability and ideal control properties in a broad range of velocities. In this subsection, OOA is applied for optimal design of permanent magnet BLDC motor with the aim of reducing loss, volume and cost. In this experiment, the OOA should find the optimal value of motor's geometric parameters such as number of pole pairs, magnet thickness and current density. Table 7 lists the minimum and maximum value of geometric parameters.

Table 7 The BLDC optimization parameters [9]

Parameters	Index	[Min Max]
Number of pole pairs	P	[1 6]
Pole–arc per pole–pitch ratio	β	[0.5 1]
Magnet thickness	l_m	[0.001 0.015]
Stator/rotor core thickness	l_y	[0.002 0.01]
Winding thickness	l_w	[0.001 0.055]
Mechanical air gap	l_g	[0.001 0.004]
Rotor radius	r_r	[0.005 0.1]
Wire gauge and stator/rotor axial length	l_s	[0.006 0.6933]
Cross sectional area of the winding	A_C	[0.1 2]
Current density	J_{CU}	[3 E 6 6 E 6]

The fitness function is a combination of motor volume (V), power loss (P) and cost of materials (C). Eq. (13) shows the fitness function. In this equation, w indicate the weight coefficient of different parts of fitness function. In the proposed motor designing algorithm, the values of w_V, w_P and w_C are 667, 0.02 and 0.0125 respectively. More details regarding test motor, geometric parameters and formulations can be found in [9].

$$F = w_V V + w_P P + w_C C \tag{13}$$

The obtained results using OOA and GA [9] are listed in Table 8. It can be seen that the proposed algorithm, OOA, has much better performance than the developed method in [9] and has led to much lower fitness function. This experiment shows that the proposed algorithm has excellent performance in solving complicated engineering problems with high dimensions and constraints.

Table 8 Obtained results by OOA and GA

Parameters	Value	
	OOA	GA [9]
P	5	5
β	0.6911	0.70
l_m	0.0122	0.0130
l_y	0.0080	0.0060
l_w	0.0032	0.00350
l_g	0.0011	0.001
r_r	0.0591	0.0595
l_s	0.0729	0.0756
A_C	1.9948	2
J_{CU}	5819700	5800000
Fitness	2.6319	2.7825

4. Conclusion

In this study, a new optimization algorithm based on orcas behavior was presented. In order to evaluate the performance of the proposed method, several benchmark functions including Schaffer, Griewank, Ackley, and Rosenbrock were used. The proposed algorithm was also used to estimate the equivalent circuit parameters of the PV module and optimal design of BLDC motor. The results of simulations and numerical studies showed that the proposed method has high accuracy and very good convergence speed, and has a much better performance than other similar algorithms such as ICA and PSO. In addition to high accuracy, the proposed algorithm has robust performance in various runs, which is an important and necessary feature for an optimization algorithm.

References

[1] D. T. Pham, and M. Castellani, "The Bees Algorithm: Modelling foraging behavior to solve continuous optimization problems," Mechanical Engineering Science, vol. 223, pp. 2919- 2938, 2009.

[2] R. Eberhart, and J. Kennedy, "A new optimizer using particle swarm theory," in Proceedings of the Sixth International Symposium on Micro Machine and Human Science, pp. 39 – 43, 1995.

[3] R. Rajabioun, F. Hashemzadeh, and E. Atashpaz-Gargari, "Colonial competitive algorithm A novel approach for PID controller design in MIMO distillation column process," International Journal of Intelligent Computing and Cybernetics, 2008.

[4] R. Rajabioun, "Cuckoo Optimization Algorithm," Applied Soft Computing, vol. 11, pp. 5508–18, 2011.

[5] A. A. Heidari, S. Mirjalili, H. Faris, I. Aljarah, M. Mafarja, and H. Chen, "Harris hawks optimization: Algorithm and applications," Future Generation Computer Systems, vol. 97, no. 3, pp. 849-872, 2019.

[6] Y, Xin-She, "Flower Pollination Algorithm for Global Optimization," 11th International Conference on Unconventional Computation and Natural Computation, Orléan, France, pp. 240-249, 2012.

[7] J. H. Holland, "Adaptation in Natural and Artificial Systems," University of Michigan Press, Ann Arbor, MI, 1975.

[8] A. Addeh, A. Khormali, and N. Amiri Golilarz, "Control chart pattern recognition using RBF neural network with new training algorithm and practical features," ISA Transactions, vol. 79, pp. 202-216, 2018.

[9] Rahideh, A., Korakianitis, T., Ruiz, P., Keeble, T., and Rothman, M. "Optimal brushless DC motor design using genetic algorithms", Journal of Magnetism and Magnetic Materials vol. 322, pp. 3680-3687, 2010.

[10] J. Addeh, and A. Ebrahimzadeh, "Breast Cancer Recognition Using a Novel Hybrid Intelligent Method," Journal of Medical Signals and Sensors, vol. 2, pp. 22-30, 2012.

[11] N. Amiri Golilarz, A. Addeh, H. Gao, L. Ali, A. Moradkhani Roshandeh, H. Mudassir Munir, and R. U. Khan, "A New Automatic Method for Control Chart Patterns Recognition Based on ConvNet and Harris Hawks Meta Heuristic Optimization Algorithm," IEEE Access, vol. 7, pp. 149398- 149405, 2019.

[12] M. Shahid, J. P. Li, N. Amiri Golilarz, A. Addeh, J. Khan, and A. Ul Haq, "Wavelet Based Image DE-Noising with Optimized Thresholding Using HHO Algorithm," 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, Chengdu, China, 2019.

[13] A. Khosravi, J. Addeh, and J. Ganjipour, "Breast Cancer Detection Using BA-BP Based Neural Networks and Efficient Features," 7th Iranian IEEE Conferences on Machine Vision and Image Processing (MVIP), Tehran, Iran, 2011.

[14] N. Amiri Golilarz, H. Gao, and H. Demirel, "Satellite image De-noising with harris hawks meta heuristic optimization algorithm and improved adaptive generalized Gaussian distribution threshold function," IEEE Access, vol. 7, pp. 57459–57468, 2019.

[15] T. Niknam, E. Taherian Fard, N. Pourjafarian, and A. Roust, "An efficient hybrid algorithm based on modified imperialist competitive algorithm and K-means for data clustering," Engineering Applications of Artificial Intelligence, vol. 24, pp. 306-317, 2011.

[16] I. N. Visser, T. G. Smith, I. D. Bullock, G. D. Green, O. GL Carlsson, and S. Imberti, “Antarctic peninsula killer whales (Orcinus orca) hunt seals and a penguin on floating ice,” Marine Mammal Science, vol 24, no. 1, pp. 225-234, 2008.
[17] National Geographic, https:// www. national geographic .com / news/2018/01/orcas-hunt-seal-antarctica-ice-video-dolphin-intelligence- whale - culture - spd/, [Accessed) October 2020]
[18] J. Ma, K. Lok Man, S. Guan, T. O. Ting, P. Wong. “Parameter estimation of photovoltaic model via parallel particle swarm optimization algorithm,” International journal of energy research, vol. 11, pp. 276-282, 2015

FAKE NEWS DETECTION USING DEEP RECURRENT NEURAL NETWORKS

TAO JIANG[1], JIAN PING LI[1], AMIN UL HAQ[1], ABDUS SABOOR[1]

[1]School of Computer Science and Engineering University of Electronic Science and Technology of China, Chengdu
E-MAIL: 3057861564@qq.com, jpli2222@uestc.edu.cn, khan.amin50@yahoo.com, saboor_khan97@yahoo.com

Abstract:

The widely spread of fake news has significantly impacted our life in politics and economics. To solve this problem, different researchers have proposed various machine learning and deep learning models. However, most of them detect fake news without desired accuracy. Therefore, we proposed a deep learning framework that classifies fake news from real ones with 99.82% accuracy. This BiLSTM model was trained and tested on a fact-checking dataset. Furthermore, we used different model evaluation metrics like precision, recall, F1-meassure, execution time to prove the efficiency of our model.

Keywords:

BiLSTM; Binary classification; Fake news detection; Deep learning

1. Introduction

Fake news has caused too many debates since the 2016 U.S. presidential election campaign. However, the human ability to detect news deception without expert assistance is quite challenging. Even fact-checking websites like Snopes.com or PoliticFact.com can only detect fake news on a small scale because the manual verification is laborious and time-consuming. We should try to solve this problem by using automatic tools to classify this news.

The task of fake news detection is usually confusing with other deception detection tasks like spam detection [1], rumor detection [2] and satire detection [3]. In this paper, we defined fake news detection as a prediction of specific news article that are fabricated intentionally to mislead people.

In some papers, researchers not only use news body to detect fake news but also combine image data, news source and comments to capture the features of fake news. In our paper, we only rely on the article text to capture the linguistic features that represents the fake news writing styles.

Khattar, et al. [4] proposed Multimodal Variational Autoencoder (MVAE) model, which used a bimodal variational autoencoder coupled with a binary classifier for the task of fake news detection. They used multimodal (textual + visual) information from popular microblogging websites: Weibo and Twitter dataset. Eventually they got 0.745 accuracy on twitter dataset and 0.824 accuracy on Weibo dataset. Their model contained three components: Encoder, Decoder and Fake News Detector which use the learned shared representation to predict. They used RNNS with LSTM cells to extract features from textual content and CNNs to train image descriptors. Shu, et al [6] developed a sentence-comment co-attention sub-network to train both news contents and user comments to jointly capture explainable top-k check-worthy sentences and user comments. Their model outperforms seven state-of-the-art fake news detection methods by at least 5.33% in F1-score, better than baselines by 30.7% in Precision. Popat, et al [7] presented DeClarE model, which aggregates signals from external evidence articles. It considered the context of the claim via word embeddings and the web articles captured via a bidirectional LSTM, while using an attention mechanism to focus on parts of the articles according to their relevance to the claim to increase interpretability.

2. Materials and methods

2.1. Data set

In [8], Ozbay et al performed more than twenty machine learning models on ISOT dataset. In this dataset, 44898 article news are contained in total, 21417 of them are real (label class is 1) and 23481 are fake (label class is 0). The dataset features include title, news body, subject, date and label. There are eight different news topics in column 'subject'. To get enough information, we combine the news body and news title to train and test our models. All text data are cleaned and tokenized before feeding them into our BiLSTM models. A little section of ISOT dataset before cleaned and after cleaned can be seen in figure1 and figure 2.

	title	text	subject	date	category
500	Senate panel votes to advance tax bill	WASHINGTON (Reuters) - The U.S. Senate Budget ...	politicsNews	November 28, 2017	1
501	Tillerson 'offended' by claims of State Depart...	WASHINGTON (Reuters) - U.S. Secretary of State...	politicsNews	November 28, 2017	1
502	Trump to make remarks at White House at 3 p.m....	WASHINGTON (Reuters) - U.S. President Donald T...	politicsNews	November 28, 2017	1
503	U.S. budget chief Mulvaney says CFPB staff sho...	WASHINGTON (Reuters) - U.S. budget chief Mick ...	politicsNews	November 28, 2017	1
504	Russian envoy to U.S. to inspect San Francisco...	MOSCOW (Reuters) - Moscow's ambassador to the ...	politicsNews	November 28, 2017	1

Fig.1 A section of uncleaned ISOT dataset

	text	category
500	WASHINGTON (Reuters) U.S. Senate Budget Commit...	1
501	WASHINGTON (Reuters) U.S. Secretary State Rex ...	1
502	WASHINGTON (Reuters) U.S. President Donald Tru...	1
503	WASHINGTON (Reuters) U.S. budget chief Mick Mu...	1
504	MOSCOW (Reuters) Moscow's ambassador United St...	1

Fig.2 A section of cleaned ISOT dataset

2.2. Bidirectional Recurrent neural networks

Deep leaning neural neworks are used in many applications [9-11]. However, bidirectional recurrent is a common variant of recurrent neural networks. It performs better on some tasks than normal RNNs and usually is used in natural language processing. RNN relies on sequence or time series to capture pattern. Therefore, when people disrupt or reverse time steps, the representations from the data can be significantly different. Based on this characteristic of RNN, bidirectional RNN like BiLSTM, are proposed. BiRNNs contain two normal RNNs, each of them processes the data in one direction and combine their representations at last. Generally speaking, bidirectional RNNs can capture some patterns that are ignored by normal RNNs.

2.3. Text tokenization

Preprocessing usually means tokenization, and weighting words in the document. To transform tokenized text into vectors, word embedding is often used. For word sequences, pretrained embedding neural networks like word2vec and glove are commonly used. In our work, we used glove to get the pretrained weighted word vectors. Considering the computation time, we limit the vocabulary to only consider the top 10000 terms across the entire corpus. We also padded every instance into 300 words long by using keras.

2.4. proposed bidirectional recurrent neural network

In the embedding layer, input_dim is the length of selected vocabulary, namely 10000. The input length is 300 just like the length of our padded instances. Output dimensionality is 100. To avoid overfitting, we also used dropout to reduce the parameters. Other detailed parameters can be seen in table 1.

Table 1 BiLSTM model structure

layer type	output shape	parameters
embedding_1	(None,300,100)	1000000
bidirectional_1	(None,300,64)	34048
bidirectional_2	(None,128)	66048
dense_1	(None,32)	4128
dense_2	(None,1)	33

2.5. Validation method

To select the best models and parameters, we used hold-out cross validation [18-19] methods on our dataset. The datasets are splited into two parts: training dataset and test dataset. Training data accounts for 80% of original dataset and the remaining data are used for testing.

2.6. Evaluation metrics

We employed different evaluation metrics to evaluate our models, such as precision, recall, accuracy and F1-meassure [12-15]. These metrics can be computed by using equations (1), (2), (3), (4).

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \text{x}100\% \quad (1)$$

$$\text{Recall} = \frac{TP}{TP+FN} \text{x}100\% \quad (2)$$

$$\text{F1-score} = 2x\frac{(precision)(recall)}{precision+recall} x100\% \quad (3)$$

$$\text{Precision} = \frac{Tp}{Tp+FP} x100\% \quad (4)$$

2.7. Proposed model procedures

The whole detection procedures are described in table 2.

Table 2 Pseudo-code of proposed fake news detection model

Step1: Begin
Step2: Pre-processing of fake news data set;
Step3: Train BiLSTM model on training data set with different parameters;
Step4: Validated BiLSTM model on testing data set;
Step5: Computes different model performance criterion;
Step6: End

3. Experimental results analysis

Our model has been trained with 80% data. The remaining essential parameters about our model have been shown in table 2. The model performance on the fake news dataset in accuracy, precision, recall, F1-meassure has been computed in table 3. The whole experiment is carried out by using python configuration of Intel Core TM i5-2410M, 4GB random access memory with 640BG hard drive, window 10. According to the results in table 3, we can see that the model performance is extraordinary. The model obtained 99.82 % accuracy, 100% recall, 100% precision, 100% F1-score. The training loss and validation loss and training accuracy and validation accuracy of our model have been shown in figure 3. The results proved that our model is of great quality and can be used to detect fake news.

Table 3 Model essential parameters

epochs	callbacks	Optimizer	loss	Output activation function
15	ReduceLROnPlateau ((monitor='val_accuracy', patience=2,verbose=1, factor=0.5,min_lr=0.001))	Adam(lr=0.01)	binary_crossentropy	sigmoid

Table 4 Model performance with multiple metrics

Accuracy(%)	precision(%)	recall(%)	F1-score(%)	Time(m)
99.82	100	100	100	50

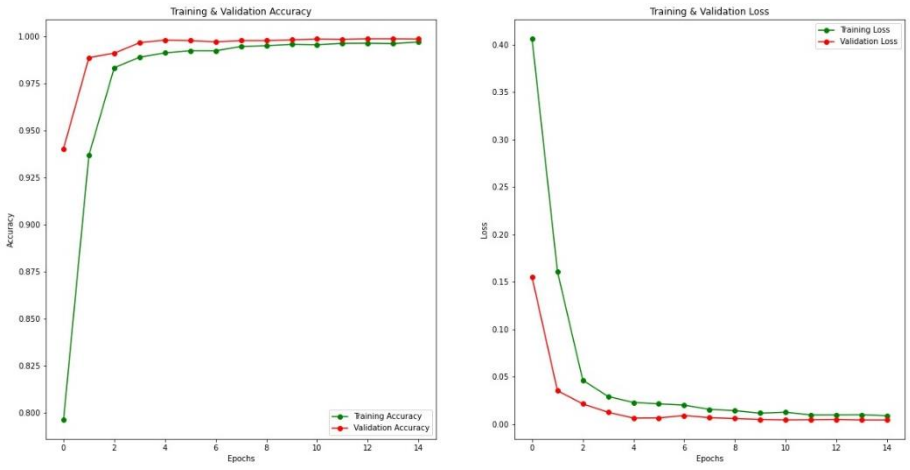


Fig 3. Model loss and accuracy curve

4. Conclusion

Our bidirectional recurrent neural network model can detect fake news with extremely high accuracy. In reality, we can use our model to automate the news validation process and help us save a lot time and free individuals from laborious fact-checking work. Our model only has two BiLSTM layers and two dense layers but achieved great performance with 99.82% in accuracy, 100% in precision,

recall and f1-score.

In future work, we may try to combine other models like CNN, GRU, LSTM with our models to see if integrated layers can improve the results. And normally speaking, data size is always the bottleneck of machine learning and deep learning tasks, so we will try to collect more data. All news in our dataset are written in English, so we also will try to apply our model in non-English dataset.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, the project of Science and Technology Department of Chongqing Municipality, Chengdu Chengdian Network Technology Co., Ltd., Chengdu Civil-military Integration Project Management Co., Ltd., and Sichuan Yin Ten Gu Technology Co., Ltd.

References

[1] Asghar, Muhammad Zubair, et al. "Opinion spam detection framework using hybrid classification scheme." Soft computing 24.5 (2020): 3475-3498.

[2] Li, Quanzhi, Qiong Zhang, and Luo Si. "Rumor detection by exploiting user credibility information, attention and multi-task learning." Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics. 2019.

[3] Toçoğlu, Mansur Alp, and Aytuğ Onan. "Satire detection in Turkish news articles: a machine learning approach." International Conference on Big Data Innovations and Applications. Springer, Cham, 2019.

[4] Khattar, Dhruv, et al. "Mvae: Multimodal variational autoencoder for fake news detection." The World Wide Web Conference. 2019.

[5] Shu, Kai , et al. "dEFEND: Explainable Fake News Detection." KDD 2019.

[6] Popat, Kashyap , et al. "DeClarE: Debunking Fake News and False Claims using Evidence-Aware Deep Learning." (2018).

[7] Ozbay, Feyza Altunbey , and B. Alatas . "Fake news detection within online social media using supervised artificial intelligence algorithms." Physica A: Statal Mechanics and its Applications 540(2020).

[8] Zhang, Malu, Hong Qu, Xiurui Xie, and Jürgen Kurths. "Supervised learning in spiking neural networks with noise-threshold." Neurocomputing 219 (2017): 333-349.

[9] Zhang, Malu, Hong Qu, Ammar Belatreche, Yi Chen, and Zhang Yi. "A highly effective and robust membrane potential-driven supervised learning method for spiking neurons." IEEE transactions on neural networks and learning systems 30, no. 1 (2018): 123-137.

[10] Zhang, Malu, Hong Qu, Ammar Belatreche, and Xiurui Xie. "EMPD: An efficient membrane potential driven supervised learning algorithm for spiking neurons." IEEE Transactions on Cognitive and Developmental Systems 10, no. 2 (2017): 151-162.

[11] Ul Haq, Amin, et al. "A novel integrated diagnosis method for breast cancer detection." Journal of Intelligent & Fuzzy Systems Preprint (2020): 1-16.

[12] Haq, Amin Ul, et al. "Feature selection based on L1-norm support vector machine and effective recognition system for Parkinson's disease using voice recordings." IEEE access 7 (2019): 37718-37734.

[13] Haq, Amin Ul, et al. "Comparative analysis of the classification performance of machine learning classifiers and deep neural network classifier for prediction of Parkinson disease." 2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP). IEEE, 2018.

[14] HAQ, AMIN UL, et al. "Identifying the Predictive Capability of Machine Learning Classifiers for Designing Heart Disease Detection System." 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing. IEEE, 2019.

[15] HAQ, AMIN UL, et al. "Identifying the Predictive Capability of Machine Learning Classifiers for Designing Heart Disease Detection System." 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing. IEEE, 2019.

RESEARCHING ON FLEXIBLE JOB-SHOP SCHEDULING PROBLEM BASED ON COMPOSITE GRASSHOPPER OPTIMIZATION ALGORITHM

DING ZHE[1,2], WU CHUNWANG[1], ZHAO JUN[1], LI BINYONG[1], LI LIANGXIAO[1], XIAN MINGZHE[1], LIAO JUNQING[1]

[1]School of Cybersecurity, Chengdu University of Information Technology, Chengdu 610225, China
[2]School of Information and software engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China
E-MAIL: dingzhe@cuit.edu.cn

Abstract:

In the practice, the essence of most scheduling problem belongs to flexible Job-Shop Scheduling problem, denoted as FJSP. As a consequence, researching for flexible job-shop scheduling has become hot spot in academy. It is difficult to directly apply traditional scheduling problems to solve FJSP because of complexity of FJSP. So, in this paper, based on grasshopper optimization algorithm, a novel algorithm is proposed and denoted as CGOA. CGOA firstly applies technology of chaotic sequence to initialize grasshopper population. And then CGOA utilizes the technology of quasi opposition-based learning, splitting strategy and Cauchy mutation to balance the ability of global search and local search. In the end, two public datasets are applied to verify the efficiency of CGOA. The result show that the efficiency of CGOA is better than traditional scheduling algorithms.

Keywords:

Flexible job-shop scheduling; Grasshopper optimization algorithm; Quasi opposition-based learning; Cauchy mutation

1. Introduction

Scheduling problem is to allocate resources for a lot of tasks in order to achieve these tasks within the stipulated time and optimize the efficiency of achieving these tasks [1]. Nowadays, the number of resources needed by achieving tasks is increasing. And the number of tasks which are simultaneously handled by scheduling system is increasing. Consequently, a lot of tasks cannot be achieved because of lacking resources. How to allocate enough resources to scheduling tasks have become a hotspot in academy [2].

Flexible Job-Shop Scheduling Problem, denoted as FJSP, is to allocate limit resources to a lot of tasks and optimize scheduling efficiency under many constraint conditions. In practice, the essence of most scheduling problem belongs to FJSP such as scheduling sources for satellite measurement and control [3-5]. Newsday, researching FJSP has become a hotspot in academy. Because of complexity, traditional scheduling algorithm cannot be directly applied to solve FJSP [6].

Based on the behavior of grasshopper foraging, Grasshopper Optimization Algorithm, denoted as GOA, was proposed by SAREMI in 2017[7]. There are two stages for searching the optimum solution of GOA. The first stage is the development stage corresponding to breadth-first search in solution space. The second stage is the exploration stage corresponding to depth-first search. During searching optimum solution, GOA limits the distance between grasshoppers in order to decrease the possibility of trapping local optimal solution.

In this paper, a novel algorithm, denoted as CGOA, is proposed to achieve FJSP. CGOA applies chaotic sequence to initialize the grasshopper population. And then CGOA utilizes the technology of quasi opposition-based learning, splitting strategy and Cauchy mutation to balance the ability of global search and local search.

2. Related works

Nowadays, many scholars have proposed a lot of algorithm to solve FJSP. ZENG proposed multi-objective optimization algorithm to solve FJSP [8]. The algorithm is based on NSGA II and applies work calendars to obtain time mechanism. And then the time mechanism is applied to achieve scheduling. Tao Ning combine quantum computing and genetic algorithm to achieve FJSP by minimizing completion time [9]. Zha Jing proposed an optimization algorithm based on hierarchical policy [10]. This algorithm can achieve FJSP by minimizing tardiness penalty cost and maximizing satisfaction. Bi Li compose simulated annealing algorithm and genetic algorithm to increase efficiency of overall researching [11].

3. Preliminaries

In order to conveniently describe the algorithm, partial mathematical symbols used in this paper are shown in table 1.

Table 1 mathematical symbols

Mathematical symbols	meaning
n	The total number of workpieces
m	The total number of machines
h_i	The total number of procedures of the ith workpiece
O_{ij}	The jth procedure of the ith workpiece
p_{ijh}	The processing time of the hth procedure of the jth workpiece in the $i$the machine.
s_{ij}	The starting time of the jth procedure of the ith workpiece
c_{ij}	The finishing time of the jth procedure of the ith workpiece
L	An enough positive number
x_{ijh}	If O_{jh} is executed in machine i, $x_{ijh}=1$, else $x_{ijh}=0$
y_{ijkl}	If O_{kl} is executed before O_{jh} in machine i, $y_{ijkl}=1$. else $y_{ijkl}=0$
C_j	Finishing time of workpiece j
f_1	Maximum finishing time
$f_1(i)$	Maximum finishing time corresponding to the ith grasshopper location
f_2	Bottleneck of machine burden
$f_2(i)$	Bottleneck of machine burden corresponding to the ith grasshopper location
f_3	Total bottleneck of all machine
$f_3(i)$	Total bottleneck of all machine corresponding to the ith grasshopper location

Flexible Job-Shop Scheduling problem is defined as follows. Given n workpieces are processed in m machines. Each workpiece has many procedures. And each procedure of a workpiece is processed in different machines. Processing order of all procedures of a workpiece is fixed. Flexible Job-Shop Scheduling problem is to find processing order and starting time of all procedures in order to minimize objective function. Three objective functions are shown from equation (1) to equation (3) [12-15].

$$f_1 = \max_{1\le j\le n} \sum_{j=1}^{n} C_j \tag{1}$$

$$f_2 = \max_{1\le i\le m} \sum_{j=1}^{n}\sum_{h=1}^{h_j} p_{ijh}x_{ijh} \tag{2}$$

$$f_3 = \sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{h=1}^{h_j} p_{ijh}x_{ijh} \tag{3}$$

Constraint conditions of flexible Job-Shop Scheduling problem are shown as equation (4) [12-13].

$$\begin{gathered} s_{ij} + x_{ijk} \times p_{ijk} \le c \\ c_{ij} \le s_{i(j+1)} \\ c_{i,h_j} \le C_{\max} \\ s_{jk} + p_{ijk} \le s_{kl} + L\left(1 - y_{ijhkl}\right) \\ c_{jk} \le s_{j,(k+1)} + L\left(1 - y_{iklj(k+1)}\right) \\ \sum_{i=1}^{m_{jh}} x_{ijh} = 1 \\ \sum_{j=1}^{n}\sum_{h=1}^{h_i} y_{ijhkl} = x_{ikl} \\ \sum_{k=1}^{n}\sum_{l=1}^{h_k} y_{ijhkl} = x_{ijh} \\ s_{jh} \ge 0, c_{jh} \ge 0 \end{gathered} \tag{4}$$

4. Proposed method

CGOA is based on grasshopper optimization algorithm to achieve FJSP. Let grasshopper population equal to N. The dimension of research space equal to D. In each iteration, location of the ith grasshopper is represented as a vector $\left(x_{i,1}, x_{i,2}, \ldots, x_{i,D}\right)$. The detail of CGOA are described as follow.

4.1. Coding for grasshopper population

The data proceed by traditional grasshopper optimization algorithm is continuous. But feasible solution of FJSP is discrete. And the feasible solution composes of machine sequence and procedure sequence. The machine sequence show executing order of procedures selected in the same machine. The procedure sequence show procedures selected for all the machines. So CGOA applies double vectors coding mechanism to code feasible solution of FJSP. The first vector represents machine sequence. The second vector represents procedure sequence.

4.2. Initialization grasshopper population

In the above section, CGOA applies double vectors coding mechanism to transform feasible solution of FJSP to vector form. In this section, CGOA applies technology of chaotic sequence to initialize grasshopper population. On the other words, CGOA applies the technology of chaotic sequence to initialized the vectors which represent feasible solutions of FJSP. The detail of initialization is described as follows [13-15].

A vector is randomly generated. The element in the vector is more than 0 and less than 1. Let the vector be $S_1 = \left(s_{1,1}, s_{1,2}, \ldots, s_{1,D}\right)\left(0 \le s_{1,i} \le 1\right)$.

Logistic equation is applied to generate N chaotic variables, shown in equation (5).

$$S_{t+1} = 4 \cdot S_t \cdot \left(1 - S_t\right), t = 1, 2, \ldots, N-1 \tag{5}$$

Equation (6) is applied to transform $S_1, S_2, \ldots, S_N$ to initial locations of all grasshoppers.

$$x_i^d = lb^d + \left(ub^d - lb^d\right) \cdot S_{id} \tag{6}$$

x_i^d is the value of dth dimension of ith grasshopper. ub^d and lb^d is upper bound and lower bound of dth dimension of grasshopper location. S_{id} is the value of dth dimension of S_i.

4.3. Updating grasshopper location

When CGOA has achieved initialization of grasshopper population, according to equation (1), equation (2) and equation (3), CGOA can obtain f_1, f_2 and f_3 of all the grasshopper locations. The optimum values of f_1, f_2 and f_3 are saved in vector $F = \left(f_1(0), f_2(0), f_3(0)\right)$.

CGOA begin to iterative operation. The detail of iterative operation is shown as follows.

obtaining optimum individual.

CGOA applies Eucil approaching degree to obtain optimum individual. The grasshopper with maximum Eucil approaching degree is the optimum individual. Let location of optimum individual be $\hat{T} = \left\{\hat{T}^1, \hat{T}^2, \cdots, \hat{T}^D\right\}$. Eucil approach degree of the ith grasshopper can be obtained by equation (7) [15].

$$F(i) = 1 - \sqrt{\sum_{j=1}^{3}\left(f_j(i) - f_j(0)\right)^2 \times \omega_j} \tag{7}$$

$$H_j = -\frac{1}{\ln 3}\left[\sum_{j=1}^{3}\left(\lambda_{ij} \ln \lambda_{ij}\right)\right] \tag{8}$$

$$\lambda_{ij} = \frac{f_j(i)}{\sum_{j=1}^{3} f_j(i)} \tag{9}$$

$$\omega_j = \frac{1 - H_j}{\sum_{j=1}^{3}\left(1 - H_j\right)} \tag{10}$$

1. updating grasshopper location

CGOA applies equation (11) to grasshopper location. Let location of the *i*th grasshopper after $\left(t+1\right)$ iterations is denoted as $X_i\left(t+1\right) = \left(x_{i,1}\left(t+1\right), x_{i,2}\left(t+1\right), \cdots, x_{i,D}\left(t+1\right)\right)$ [7].

$$x_{i,d}\left(t+1\right) = c_i\left(\sum_{j=1, j\ne i}^{N} c_i \frac{ub^d - lb^d}{2} s\left(d_{ij}\left(t\right)\right) \frac{X_j\left(t\right) - X_i\left(t\right)}{d_{ij}\left(t\right)}\right) + \hat{T}^d \tag{11}$$

$$s\left(d_{ij}\left(t\right)\right) = f \cdot \exp\left(\frac{-d_{ij}\left(t\right)}{l}\right) - \exp\left(-d_{ij}\left(t\right)\right) \tag{12}$$

$$d_{ij}\left(t\right) = \left|X_j\left(t\right) - X_i\left(t\right)\right| \tag{13}$$

$$c_i = \begin{cases} c\min + \dfrac{\left(c\max - c\min\right) \cdot \left(F(i) - F_{\min}\right)}{F_{avg} - F_{\min}} & F(i) \le F_{avg} \\ c\max & F(i) > F_{avg} \end{cases} \tag{14}$$

$X_j\left(t\right)$ is the *j*th grasshopper's location after *t* iterations.

Traditional grasshopper optimization algorithm applies a linear strategy to adjust a parameter *c* which is used to balance global search and local search. When traditional grasshopper optimization algorithm is applied to solve FJSP, the algorithm falls into a local optimal solution. In this paper, nonlinear inertia weight is applied to balance global search and local search. For *i*th grasshopper, the nonlinear inertia weight for the *i*th grasshopper can be denoted as c_i and can be obtained by equation (14) [19]. $F(i)$ is Eucil approaching degree of *i*th grasshopper. F_{avg} is mean value of Eucil approaching degree of all grasshoppers. $F_{\min}$ is minimum value of Eucil approaching degree of all grasshoppers. $c\min$ and $c\max$ are minimum and maximum values of *c* used in grasshopper optimization algorithm.

2. Optimizing grasshopper location

When CGOA obtain all the grasshopper locations, CGOA applies quasi opposition-based learning and the idea of celestial body to optimize these grasshopper locations.

Quasi opposition point of $x_{i,j}\left(t+1\right) \in X_i\left(t+1\right)$ is denoted as $x_{i,j}^{qo}\left(t+1\right)$ and can be obtained by equation (15) [16].

$$x_{i,d}^{qo}\left(t+1\right) = rand\left(\frac{ub^d + lb^d}{2}, ub^d + lb^d - x_{i,j}\left(t+1\right)\right) \tag{15}$$

$rand(a,b)$ is a random number which belongs to a range between a and b.

Let $X_i^{qo}(t+1)=\left(x_{i,1}^{qo}(t+1),x_{i,2}^{qo}(t+1),\cdots,x_{iD}^{qo}(t+1)\right)$ is Guasi opposition location of $X_i(t)$. CGOA can obtain Eucil approaching degrees of $X_i(t+1)$ and $X_i^{qo}(t+1)$. The most value of Eucil approaching degree corresponding to location is the optimized location of the ith grasshopper after t iterations.

When CGOA obtains optimized location of the ith grasshopper after t iterations, CGOA applies the idea of splitting celestial body to ensure final location after i iterations. Let $\tilde{X}_i(t+1)$ is the optimized location of the ith grasshopper after t iterations. CGOA applies inequation (15) to judge whether $\tilde{X}_i(t+1)$ satisfies the condition of splitting celestial body [17-18].

$$\frac{d_{i,k}}{d_{i,\hat{T}}}<C \tag{16}$$

$$C=C_0\left(1-\frac{t}{T}\right) \tag{17}$$

$d_{i,k}$ is the distance between the ith grasshopper and the kth grasshopper whose location is closest with the ith grasshopper. $\hat{T}$ is the location of the optimum individual after t-1 iterations. T is the maximum number of iterations.

When the ith grasshopper satisfies the condition of splitting celestial body, CGOA applies equation (18) to obtain splitting location [17, 18], denoted as $\tilde{X}_i'(t)$.

$$\tilde{X}_i'(t+1)=\frac{t}{T}X_i(t+1)+\left(1-\frac{t}{T}\right)\cdot X_I(t+1)\cdot D \tag{18}$$

$$D=\begin{cases} d_{i,k}\times rand\left(-\frac{1}{2},\frac{1}{2}\right) & d_{i,k}\geq e^{-t/T} \\ d_{i,k}+rand\left(-\frac{d_{i,k}}{2},\frac{d_{i,k}}{2}\right) & otherwise \end{cases} \tag{19}$$

And then CGOA can obtain Eucil approaching degrees of $\tilde{X}_i(t+1)$ and $\tilde{X}_i'(t+1)$. The most value of Eucil approaching degree corresponding to location is the final location of the ith grasshopper after t iterations.

3. Optimization of optimum individual

When optimum individual has not changed during t+1 iterations, CGOA maybe fall into local optimization optimum. So, CGOA applies Cauchy mutation to avoid local optimization optimum.

Let $\hat{T}(t)=\left\{\hat{T}^1(t),\hat{T}^2(t),\cdots,\hat{T}^D(t)\right\}$ is the location of the optimum individual after t iterations. CGOA applies equation (20) to obtain mutation location of the optimum individual, denoted as $\tilde{T}(t)=\left\{\tilde{T}^1(t),\tilde{T}^2(t),\cdots,\tilde{T}^D(t)\right\}$ [19-20].

$$\tilde{T}^d(t)=\hat{T}^d(t)+F_t\cdot C\left(lb^d,ub^d\right) \tag{20}$$

$$F_t=\left(\frac{T-t}{T}\right)^2 \tag{21}$$

CGOA applies Eucil approaching degrees of $\hat{T}(t)$ and $\tilde{T}^d(t)$ to ensure optimum individual.

The process of CGOA is shown as follow.

4. CGOA initializes the parameters and applies equation (5) and equation (6) to initialize grasshopper population.

5. CGOA applies equation (1), equation (2) and equation (3) to obtain the values of f_1, f_2 and f_3. And then CGOA applies Eucil approaching degree to obtain optimum individual, shown as equation (7).

1) In $(t+1)$ th iteration, for the ith grasshopper, CGOA applies equation (11) to obtain the location of the *i*th grasshopper, denoted as $X_i(t+1)$. And then CGOA applies Quasi opposition-based learning to obtain Guasi opposition location of *i*th grasshopper, denoted as $X_i^{qo}(t+1)$, shown as equation (15). According to Eucil approaching degrees, CGOA can obtain the optimized location of the *i*th grasshopper after *t*+1 iterations. Finally, COGA applies equation (16) to judge whether the optimized location satisfies the condition of splitting the celestial body. If the optimized location satisfies the condition of splitting celestial body, CGOA applies equation (18) to obtain the splitting location of the optimized location. And according to Eucil approaching degrees, CGOA can obtain the final location of the ith grasshopper after t+1 iterations.

2) CGOA return 2) step until obtaining an optimum result. If the optimum individual has not changer during k iterations, CGOA applies Cauchy mutation to update optimum individual, shown equation (20).

5. Performance evaluation

OR-Library dataset is applied to verify the efficiency of CGOA. The detail of this dataset can be obtained in http://people.brunel.ac.uk/~mastjjb/jeb/orlib/files/jobshop1.txt. In this paper, we choose FT dataset and LA dataset from OR-Library. And FT dataset and LA dataset are usually used to verify the efficiency of scheduling algorithm.

The operating environment of the experiments is python 3.8, Intel Core i5 CPU, 4G of memory. The parameters in CGOA are set as follow. The number of grasshopper population is equal to 200. Maximum number of iterations is

equal to 300. The values of cmax and cmin are equal to 1 and 0.001, respectively. Contrast algorithms are denoted as MDPS [21] and HGA [22].

We run the three algorithms 30 times. According to the results of minimize f_1, f_2 and f_3, we have obtained meaning value of meaning running result Δ_{avg}, the meaning value of maximum running result Δ_{max}, the meaning value of minimum running result Δ_{min} and meaning variance of running result Δ_{std}. The results are shown as table 3.

The results show that the efficiency of CGOA is better than other algorithms. When the scale of the problem is small, CGOA, MDPS and HGA can find good scheduling schemes. Gantt Chart of FT06 and LA01 for CGOA are shown in Fig 1 and Fig 2. But the efficiency of scheduling scheme obtained by CGOA is better than other algorithms. When the scale of the problem becomes large, the efficiency of CGOA is far better than the other algorithms. The reason is that MDPS and HGA fall into a local optimum solution. CGOA applies technology such as Quasi opposition-based learning and Cauchy mutation to balance global search and local search. As a result, CGOA avoids local optimal solution and increases the convergence rate. And CGOA applies the technology of chaotic sequence to reduce the adverse impact of initialization.

Table 3 Experiment results

instance	Problem Size	CGOA				MDPS				HGA			
		Δ_{min}	Δ_{max}	Δ_{avg}	Δ_{std}	Δ_{min}	Δ_{max}	Δ_{avg}	Δ_{std}	Δ_{min}	Δ_{max}	Δ_{avg}	Δ_{std}
FT06	6 × 6	41.2	60.2	52.8	0.8	54.2	63.4	56.2	1.2	52.1	61.4	56.03	0.95
FT10	10 × 10	971.3	1132.5	992.4	38.4	1023.4	1342.3	1124.8	35.4	1003.2	1432.2	1261.3	34.6
FT20	20 × 5	904.7	1524.6	1249.2	36.1	1158.6	1673.2	1255.4	33.7	1241.2	1734.2	1564.2	46.3
LA01	10 × 5	585.6	780.4	670.7	9.6	593.4	801.7	684.7	11.6	603.8	823.5	694.1	13.5
LA06	15 × 5	875.2	1009.3	926.2	2.5	901.4	1105.2	934.6	1.3	903.8	1109.8	935.2	5.3
LA11	20 × 5	1004.2	1443.8	1221.3	0.27	1230.2	1521.6	1334.1	0.7	1023.6	1643.2	1375.8	0.32
LA16	10 × 10	883.6	1002.6	978.2	25.8	1285.6	1535.7	1352.6	21.9	913.2	1274.4	1104.8	24.6
LA21	15 × 10	982.6	1298.6	1183.3	36.2	1035.3	1643.8	1352.3	29.6	990.7	1398.4	1253.6	32.7
LA26	20 × 10	1016.2	1498.6	1398.2	73.8	1293.4	1743.9	1534,6	63.5	1075.3	1687.3	1573.2	62.9
LA31	30 × 10	1698.2	2013.5	1894.7	49.3	1896.5	2215.3	2014.8	41.6	1734.8	2486.4	2143.2	45.9
LA36	15 × 15	1144.2	1534.7	1453.6	68.4	1423.6	1895.2	1643.7	68.2	1253.2	1643.8	1533.7	63.3

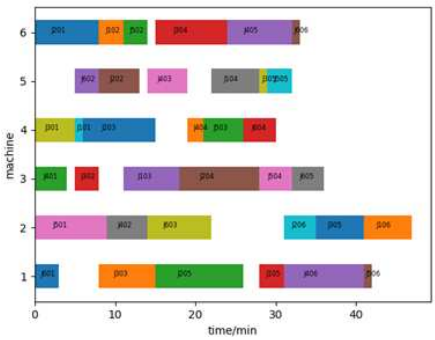


Fig.1 Gantt Chart of FT06

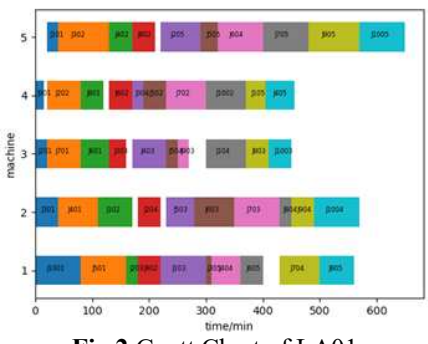


Fig.2 Gantt Chart of LA01

Acknowledgements

This paper is supported by Sichuan Science and Technology Program (No. 2019YFG0425, 2019YFG0408); The open Project of Network and Data security Key Laboratory of Sichuan Provence (No. NDS2018-1); the National Natural Science Foundation of China (Grant No.71701026);

References

[1] Lin T L, Horng S J, Kao T W, et al. An efficient job-shop scheduling algorithm based on particle swarm optimization[J]. Expert Systems with Applications an International Journal, Vol 37, No. 3, pp.2629-2636, 2010.

[2] Li C, Tang J, Ma T, et al. Load balance-based workflow job scheduling algorithm in distributed cloud[J]. Journal of Network and Computer Applications, Vol 152, pp. 1025-1043, 2019.

[3] Wanlin Y. Research on Multi-objective Dynamic Scheduling Optimization in Flexible Job Shop[D], Southwest University of Science and Technology，2018.

[4] Jin Feng Wang, Bi Qiang Du, Hai Min Ding. A genetic algorithm for the Flexible Job-shop Scheduling Problem[M]. Advanced Research on Computer Science and Information Engineering. Springer Berlin Heidelberg, 2011.

[5] Wu X, Wu S. An elitist quantum-inspired evolutionary algorithm for the flexible job-shop scheduling problem[J]. Journal of Intelligent Manufacturing, Vol 28, No. 6, pp. 1441-1457, 2017.

[6] Chenglong W, Cheng, Li, Yiping Fen. Dispatching rule extraction method for job shop scheduling problem[J]. Journal of Zhejiang University (Engineering Science), Vol 49, No. 3, pp. 421-429, 2015.

[7] Meng X . Grasshopper optimization algorithm for multi-objective optimization problems[J]. Computing Reviews, Vol 60, No. 5, pp. 214-224, 2019.

[8] Qiang Z, Menghui C, Menghua W, et al. Multi-objective optimization method for FJSP under mixed work calendars[J]. Journal of Chongqing University, 2019.

[9] Ning T, Jin H, Song X, et al. An improved quantum genetic algorithm based on MAGTD for dynamic FJSP[J]. Journal of Ambient Intelligence & Humanized Computing, 2017.

[10] Jing Z, Hua J, Zhengjia W, et al. Solving integrated optimization of equipment maintenance and FJSP based on hierarchical biogeography-based algorithm[J]. Modern Manufacturing Engineering, 2018.

[11] Li B, Jin B F. Research on Dynamic Multi-objective FJSP Based on Genetic Algorithm[C]. 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing. IEEE Computer Society, 2018.

[12] Lei Cao, Chunming Ye, Xia Huang. Multi-objective flexible Job-Shop scheduling based on variable neighborhood search invasive weed optimization[J]. Application Research of Computer, 2018, Vol 35; No.315, pp. 156-171, 2018.

[13] Li Zhang. Research on Flexible Job-Shop Scheduling Problem Based on Multi-objective Optimal Algorithm[D]. SHANGDONG AGRICULTURAL UNIVERSITY, 2019.

[14] Jing Z, Hua J, Zhengjia W, et al. Solving integrated optimization of equipment maintenance and FJSP based on hierarchical biogeography-based algorithm[J]. Modern Manufacturing Engineering, 2018.

[15] Xia Huang, chunming Ye, Lei Cao. Composite mutation invasive weed optimization algorithm for multi-objective Job-Shop scheduling proble[J]. Application Research of Computer, No. 12, pp. 113-132, 2017.

[16] S. Rahnamayan, H. R. Tizhoosh, M. Salama. Quasi-oppositional differential evolution[C]. IEEE Congress on Evolutionary Computation, pp. 2229-2236, 2007.

[17] Hao Liu. Researches of Diversity Enhanced Particle Swarm Optimization and Its Application[D]. BEIJING INSTITUTE OF TECHNOLOGY. 2015.

[18] Sarafrazi S, Nezamabadi-Pour H, Saryazdi S. Disruption: A new operator in gravitational search algorithm[J]. Scientia Iranica, Vol 18, No. 3, pp. 539-548, 2011.

[19] Lanlan Kang. Several Improvements to Particle Swarm Optimization and Their Theoretical Fundamentals[D]. Wuhan university. 2017.

[20] Jinjie Wang. Research and Application of Multi-objective Particle Swarm Optimization Algorithm[D]. Anhui University,2020.

[21] Huang S, Tian N, Wang Y, et al. Multi-objective flexible job-shop scheduling problem using modified discrete particle swarm optimization[J]. Springerplus, Vol 5, No. 1, pp. 1432-1442, 2016.

[22] Huang X, Yang L. A hybrid genetic algorithm for multi-objective flexible job shop scheduling problem considering transportation time[J]. International Journal of Intelligent Computing and Cybernetics, Vol 12, No. 2, pp. 154-174, 2019.

APPLYING CNN WITH EXTRACTED FACIAL PATCHES USING 3 MODALITIES TO DETECT 3D FACE SPOOF

KUUPOLE ERUBAAR EWALD[1]*, LIAOYUAN ZENG[1], ZHENG YAO[1], COBBINAH BERNARD MAWULI[1], HASSAN SANI ABUBAKAR[1], AGBESI VICTOR[1]

[1] University of Electronic Science and Technology of China, China.
E-MAIL: ewaldkuupole@gmail.com, lyzeng@uestc.edu.cn

Abstract:

In an era of smart technology where the human face is used for authentication because its fast and convenient but not every technology introduced is 100% credible. Face spoofing has rendered this technology vulnerable because of the damage it can cause when its security is breached. 3D face spoof has emerged and complicated facial recognition systems. Although, sophisticated improvement over the years have been made to reduce the impact of 3D face spoofing, a robust solution that can change the facial recognition sensors from being fooled are still studied and been researched on. In this paper, we proposed a (Convolutional Neural Network, CNN) architecture focused on Fusion-based approach, Depth and Patch-based (Convolutional Neural Network, CNN) by extracting from the human facial images, the facial features and complete detail hints. Our tests were carried out on CASIA-SURF dataset consisting of 3 modalities: Color, Depth and (Infrared, IR).

Keywords:

Face Spoofing; Patch-Based CNN; Depth-Based CNN; Fusion-Based CNN

1. Introduction

Fingerprint was used in the 1880s as the easiest way to recognize merchants, kids etc.by the Babylonians and the Chinese by applying ink to the finger and applying onto a paper for identification it was regarded as the best suitable way due to unique fingerprints but it was bulky and takes time to find a match [1][2]. Facial recognition is a biometric software which is able to uniquely able to verify an individual by comparing and evaluating facial cues depicting a person's face [3]. It is regularly used for security aspects, there is an increasing attention in other areas where facial recognition is applied.

Spoofing attacks to the biometric systems has greatly affected in verifying the identity of an individual [4]. Detection of the spoofing attacks is a stern problem although facial recognition systems and voice verification systems are mostly weak to spoofing [5][6].

Depth-Based CNN: If we have a CNN. One single convolution operation would be pointless since it used for the entire image depiction it can specify, but only to specific features situated on the face or an object [7] [8]. In depth-based CNN it is believed that high-frequency information of facial images is very important for spoof detection and reducing the quality of an image(s) will deteriorate the value of the image(s) so to prevent this this from happening maintaining the original image(s) size in CNN training for the depth approximation [9]. By training a completely FCN (Fully Convolutional Network) whose constraints are independent depending on the image(s) scale of the facial data, the data is facial image(s) and the output is the corresponding maps of the depth [10].

1.1. Contributions

- We proposed a new Fusion-Based approach to effectively merge 3 input modalities; Color, Depth and IR to detect a real face from a spoofed face.
- The proposed Fusion-Based approach robustly extracts the characteristics of a spoofed face and detects facial recognition attacks. The anti-spoof face detection task is explored by applying different deep learning techniques to ascertain its effects on the models' performance.
- We achieve the state-of-the-art performance on conventional face anti-spoofing CASIA-SURF dataset by utilizing both learned local and global features in generalizing the detection of live and spoofed face using extracted facial patches.

2. Proposed Method

Dataset: On the basis of our proposed method, we test our experiment using CASIA-SURF [11] popular dataset for the detection of 3D facial patch spoof. CASIA-SURF: This dataset includes 300 training images in which each sample has range of 20 to 50 images for Color, Depth and IR image samples. This dataset uses 300 images for training, 10 subjects for validation and 30 subjects for testing.

The Architectural Model: We suggest a methodology using,

- Patch-Based CNN [9], Depth-based CNN [12]; a high-level CNN preparation and Fusion process to assess our real and fake faces respectively. We achieved our aim for the CNN Patch-Based by training a deep end-to-end neural network to learn features of rich appearance that can distinguish between a live and spoofed facial image by randomly extracting patches from the facial images of a person [13] [14]. For both reasons the fusion approach has achieved positive performance outcomes. We'll point to the spoof score as our success on fusion. Figure 3 provides an example for color and patch along with a fusion approach.
- We trained a deep, end-to-end neural network to learn salient features for the Patch-Based CNN medium, which can distinguish between a live and a spoofed facial image using the patches extracted from the human facial image dataset. We trained a FCN for the Depth-Based CNN source to estimate the depth of a facial image, thinking a print or replay projection attack had a flat depth chart, whereas live faces have a natural depth of face sometimes referred to as 3D. Face-attacks can be identified separately either by the presence or distance cues. Fusing all signals has proved to produce promising results, however. Throughout our research, we refer to the final recorded spoof-score as the fusion performance.
- Depth-Based CNN one single convolution operation would be pointless in a CNN architecture since it is used for the entire image representation it can specify, but only for specific features on the face or object [10]. In depth-based CNN, high-frequency facial image knowledge is considered to be very critical for spoof identification, so reducing the quality of an image(s) would deteriorate the image(s) quality [9][16]. To avoid this from happening, it is advised that the original image(s) size be preserved for approximation of depth in the CNN instruction. By training an FCN whose restrictions are independent of the scale of the facial image(s) of the origin, the image(s) of the facials and output must correspond to the maps of the distance. In comparison, 3D-mask PA also called PAs, such as a printed paper and show, clearly have a different dimension compared to the live face [7][9].

CNN Architecture for Fusion Based Modality: In the fusion-based CNN architecture, we modelled three (3) distinct architecture for Color, Depth, and IR data respectively, to achieve the proposed fusion-based configuration, the architectures were concatenated at the previous convolutional layer of each model. Using the Residual Network (ResNet) method, the convolution layers of each model are modelled. That each block of the residual network contains at least 2 layers of convolutional neural network, the design of each image modality we mentioned below:

1. Color-based CNN architecture: There is a total of six (6) convolutional layers in this design. A ReLU activation feature is accompanied by a single convolutional layer. A Maxpooling is accompanied by production of the first, second, fourth and sixth convolutional neural layers. The number of filters for each convolutional layer are 64,64,128,128,256 and 512 respectively. We also ensured that batch normalization and max pooling were respectively pursued on each convolutional layer. The performance of this network is concatenated with the data for fusion dependent implementation of the Depth-based and IR-based CNN architectures.

2. Depth-based CNN architecture: In total this architecture has six (6) convolutional layers. An activation feature for ReLU is also accompanied by a convolutional layer. A Maxpooling is accompanied by production of the first, second, fourth and sixth convolutional neural layers. For increasing convolutional layer, the number of filters is 64,128,128,256,256 and 512, respectively. We also ensured that batch normalization and max pooling were respectively pursued on each convolutional layer. The data of this network is concatenated with performance of the fusion-based application of the Color and IR-based CNN architectures.

3. IR-based CNN architecture: This architecture, has a total of Seven (7) convolutional layers. The convolutional layer is followed by a ReLU activation function. The output of the first, fourth, sixth and seventh convolutional neural layers is followed by a max pooling. The number of filters for each convolutional layer are 64,128,128,256,256,256 and 512 respectively. Also, we ensured that each convolutional layer was followed by batch normalization and max pooling respectively. The output of this network is concatenated with the output of the Color and Depth-based CNN architectures for the fusion based implementation.

4. Fusion: The output of the Color, Depth and IR-based CNN architecture are concatenated and followed by 2 blocks of residual neural network, an average pooling, a dropout, 2 fully connected layers. The basic components of the residual neural network are 2 convolutional layers with each having a kernel size of 3 and a stride of 1. Each convolutional neural

network has a ReLU activation function. The first fully connected layer has 512 neuron and the last fully connected serving as the class prediction output (Real vs Fake). Figure 1 and table 1 represents the architecture in detail.

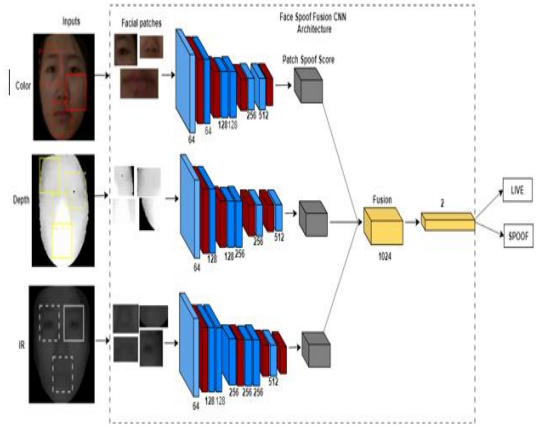


Fig.1 Showing the Fusion CNN Architecture.

3. Results and Discussion

Evaluation Metric: The efficacy of the suggested CNN face spoof architectures was analyzed and measured using the criteria for the accuracy test. For a given set of data instances, let TP, FP, FN and TN mean the number of true positive, false positive, false negative and true negative classification tests, respectively. A standard classification function efficiency is calculated using the following metrics: accuracy; responsiveness or recall; specificity; described in the following equations:

$$Accuracy = \frac{TP+TN}{TP+TN+FN+FP}, \quad (1)$$

$$Sensitivity = \frac{TP}{TP+FN}, \quad (2)$$

$$Specificity = \frac{TN}{TN+FP} \quad (3)$$

$$F1 = 2 \text{ x } \frac{\text{Precision} * \text{Recall}}{Precison+Recall} \quad (4)$$

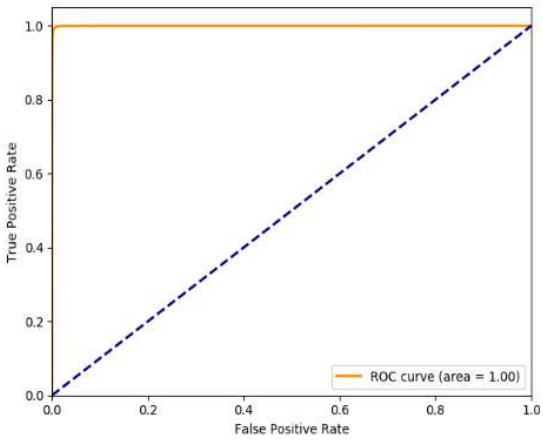
Results on CNN architecture for Color, Depth and IR modality: The architecture of the color, depth and IR modality comprises of 6 convolutional layers, and each convolutional layer is followed by a ReLU[15] activation function. A max pooling is followed by the output of the first, second, fourth and sixth convolutional neural layers. The use of strides in convolutional neural networks is to let the network learn its own spatial down sampling. As the height, width and depth of the CASIA-SURF dataset images are progressively reduced along the layers, number of filters in the successive layers are increased. We increased the filters so that we can compensate for the information losses during the down sampling operation. The output of the last convolution the fusion spoof score is attained. The network is trained using SGD with a learning rate of 0.1, epoch of 100.

Table 1 Hyperparameter Values for the Proposed Models Training.

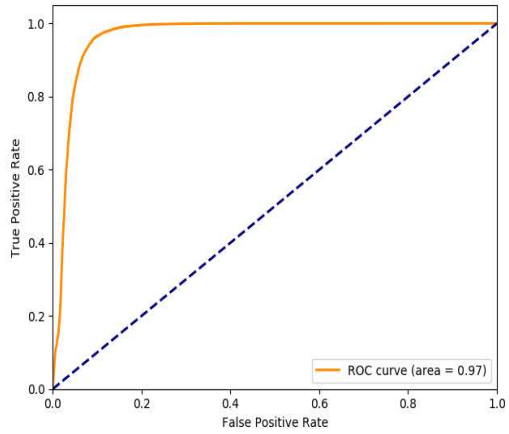
	Learning Rate	**Epoch**	**Optimizer**
CNN Architecture for Color modality	0.1	100	SGD
CNN Architecture for Depth modality	0.1	100	SGD
CNN Architecture for IR modality	0.1	100	SGD
CNN Architecture for Combined modality	0.1	100	SGD
Fusion CNN Architecture for Combined modality	0.01	100	Adam
CNN Architecture for Single modality	0.1	100	SGD
SGD= Stochastic Gradient Descent			

Table 2 Test Accuracy on CNN architecture for Color, Depth and IR modality.

	Training Accuracy	Validation	Testing	F1 Score
Color	0.856	0.876	0.852	0.884
Depth	0.991	0.999	0.990	0.996
IR	0.971	0.896	0.896	0.921



(a)



(b)

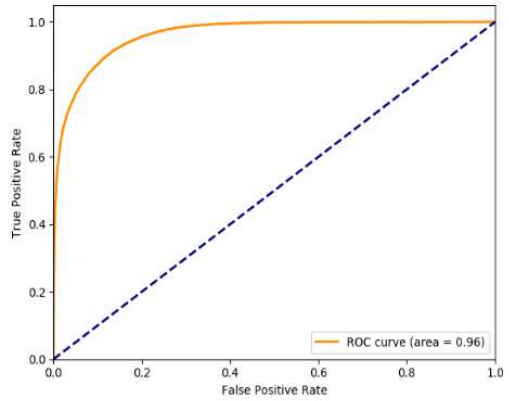


Fig.2 ROC curves for (a) Color, (b) Depth and (c) IR modality.

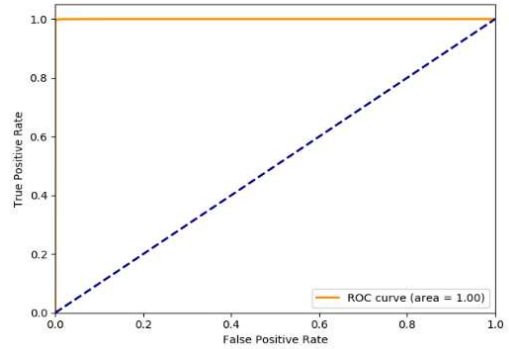


Fig.3 ROC curve for Fusion CNN architecture for combined modality.

Discussion of Results: From our experiment, the following conclusions can be drawn:

1. Fusion approach seems to be a viable deep learning way of classifying 3 image inputs (Color, Depth and IR dataset) without Preprocessing. It has the capability of bringing the 3 different inputs and extracting the relevant patches of the human face and determining which face is fake or real.
2. With the exception of the architecture pretrained with CNN we conclude our proposed Fusion based architecture performed better than the single architectures.
3. In this experiment we applied cosine annealing restart of both Adam and Stochastic Gradient Descent optimizers (SGD)[24]. The main objective behind this technique is to prevent the issues of disappearing gradient when training deep learning models and select the best optimized learning rate[16][17].
4. From the perspective of IR modality, it could be seen that the binary classification of Color is more difficult task as compared to IR and Depth.
5. The observed ROC curve from the experimental results indicates that the combined dataset for a single deep learning CNN architecture is a challenging task and is even more challenging when there is no initial data Preprocessing pipeline.
6. The results presented in this work are encouraging from the perspective that the Fusion methodology used for Color, Depth and IR 3D face spoof with depth and patch-based deep learning CNN architecture were not preprocessed and has a higher accuracy, ROC and F1 score.
7. The results obtained by the Fusion model as seen in the table proves to be the best with a ROC score of 1.00 and an F1 score of 0.998, even though the Single depth model matched the ROC score of the Fusion. We observed that it's F1 score value was lesser as compared to the Fusion.

Table 3 Provides the summary of the performance of the various 3D face spoof architectures with its data modality.

	Accuracy	**ROC**	**F1 Score**
Color modality model	0.852	0.96	0.884
Depth modality model	0.990	**1.00**	0.996
IR modality model	0.896	0.97	0.921
Combined model	0.392	0.69	0.489
Fusion model	**0.997**	**1.00**	**0.998**

Solution Comparison: We present a review comparison on extracted facial patches to detect 3D face spoof consisting of Color, Depth and IR dataset. The table below shows some of the state-of-the-art results of 3D face spoof attack. Almost all 3D face spoof research results have different results and methodology approaches used to achieve their results. This enabled us to make a holistic comparison with our work.

Table 4 Comparison review with existing work's methods and accuracy scores.

Method	Data set	Subject	F1 Score	Modality	Training Accuracy	Validation Accuracy
SVM EBF [18]	CASIA	75	0.890	RGB	0.90	0.89
Spoof ResNet [19]	MSU-MFSD	35	N/A	RGB	0.978	0.944
MTCNN [20]	YOUTU	3350	0.956	RGB/IR	0.962	0.978
SqueezeNet [21]	CASIA-SURF	1000	N/A	Color, Depth & IR	N/A	0.998
FusionNet	CASIA-SURF	300	**0.998**	Color, Depth & IR	**0.997**	**0.998**

4. Conclusion

In this research, we used a deep learning method focused on Fusion CNN architecture to derive facial patches and depth of 3 types of human facial image samples namely Color, Depth and IR from the CASIA-SURF dataset modeled with an altered 3D convolutional neural network classifier. Our primary interest was to be able to extract facial patches and the depth levels of all 3 facial inputs stated earlier on to distinguish a real face from a spoofed face from a CASIA-SURF dataset provided which are not preprocessed.

Acknowledgements

This work is supported by Department of Science and Technology of Sichuan Province, China, under Grant 2019YJ0166.

References

[1] J. Berry and D. A. Stoney. The history and development of fingerprinting [J]. Advances in fingerprint Technology, 2001, 2:13–52.

[2] W. Yang, S. Wang, J. Hu, et al. Security and accuracy of fingerprint-based biometrics: A review [J]. Symmetry, 2019, 11(2):141.

[3] L. Introna and H. Nissenbaum. Facial recognition technology a survey of policy and implementation issues [J].2010.

[4] D. Wen, H. Han, and A. K. Jain. Face spoof detection with image distortion analysis [J]. IEEE Transactions on Information Forensics and Security, 2015, 10(4):746–761.

[5] K. A. Nixon, V. Aimale, and R. K. Rowe.Handbook of biometrics, 2008, 403–423.

[6] A. da Silva Pinto, H. Pedrini, W. Schwartz, et al. Video-based face spoofing detection through visual rhythm analysis [C].2012 25th SIBGRAPI Conference on Graphics, Patterns and Images, 2012, 221–228.

[7] A. Krizhevsky, I. Sutskever, and G. E. Hinton. Imagenet classification with deep convolutional neural networks [C]. Advances in neural information processing systems, 2012, 1097–1105.

[8] Y. Atoum, Y. Liu, A. Jourabloo, et, et, et al. Face anti-spoofing using patch and depth-based CNNs [C].2017 IEEE International Joint Conference on Biometrics (IJCB), 2017, 319–328.

[9] R. Min, J. Choi, G. Medioni, et al. Real-time 3D face identification from a depth camera [C]. Proceedings of the 21st International Conference on Pattern Recognition (ICPR2012), 2012, 1739–1742.

[10] S. Lawrence, C. L. Giles, A. C. Tsoi, et al. Face recognition: A convolutional neural-network approach [J]. IEEE transactions on neural networks, 1997, 8(1):98–113.

[11] Z. Zhang, J. Yan, S. Liu, et al. A face antispoofing database with diverse attacks [C].2012 5th IAPR international conference on Biometrics (ICB), 2012, 26–31.

[12] G. Albakri and S. Alghowinem. The effectiveness of depth data in liveness face authentication using 3D sensor cameras [J]. Sensors, 2019, 19(8):1928.

[13] J. Dai, Y. Li, K. He, et al. R-fcn: Object detection via region-based fully convolutional networks [C]. Advances in neural information processing systems, 2016, 379–387.

[14] C.-L. Zhang, J.-H. Luo, X.-S. Wei, et al. In defense of fully connected layers in visual representation transfer [C]. Pacific Rim Conference on Multimedia, 2017, 807–817.

[15] J. Konečny, J. Liu, P. Richtárik, et al. Mini-batch semi-stochastic gradient descent in the proximal setting [J]. IEEE Journal of Selected Topics in Signal Processing, 2015, 10(2):242–255.

[16] A. F. Agarap. Deep learning using rectified linear units (relu) [J]. arXiv preprint arXiv:1803.08375, 2018.

[17] L. Bottou.Neural networks: Tricks of the trade, 2012, 421–436.

[18] M. Hardt, B. Recht, and Y. Singer. Train faster, generalize better: Stability of stochastic gradient descent [J]. arXiv preprint arXiv:1509.01240, 2015.

[19] D. T. van der Haar. Face Antispoofing Using Shearlets: An Empirical Study [J]. SAIEE Africa Research Journal, 2019, 110(2):94–103.

[20] C. Nagpal and S. R. Dubey. A performance evaluation of convolutional neural networks for face anti spoofing

[C].2019 International Joint Conference on Neural Networks (IJCNN), 2019, 1–8.
[21] A. Ghofrani, R, R. M. Toroghi, and S. M. Tabatabaie. Attention-Based Face AntiSpoofing of RGB Images, using a Minimal End-2-End Neural Network [J]. arXiv preprint arXiv:1912.08870, 2019.
[22] A. Liu, J. Wan, S. Escalera, et al. Multi-modal face anti-spoofing attack detection challenge at cvpr2019 [C]. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2019, 0.

IMPROVED IMAGE DEBLURRING ALGORITHM TO GENERATE ANTAGONISTIC NEURAL NETWORK

ZOU QIANYING[1], LUO LAN[1], WANG XIAOFANG[1], CHEN DONGXIANG[1], LIU FENGYU[1]

[1]Chengdu Colleges of University of Electronic Science and Technology of china, Sichuan, Chengdu,611731, China
E-MAIL: 939549393@qq.com

Abstract:

Aiming at the difficulty of the de-blurring kernel, poor de-blurring effect, and ringing caused by image noise in the traditional de-blurring method of moving image with the fuzzy kernel, a new algorithm based on edge discrimination and antagonistic neural network is proposed in this paper. The improved algorithm is based on the traditional condition to generate the antagonistic neural network by reducing the noise of the blurred image, extracting the edge information of the image and using it as the auxiliary information to guide the de-blurring effect in the generator. The discriminator network is improved, that is, two discriminators are used to distinguish the de-blurred image and the edge image extracted from the de-blurred image, and the two discriminators must be deceived simultaneously to achieve the de-blurring effect. Compared with the end-to-end deblurring algorithm in recent years, in the image dataset with 0.007 Gaussian noise, the PSNR of the improved algorithm is increased by 7.7% and the structural similarity is increased by 10% on average, but its running time is unchanged. Experimental results show that the improved algorithm can effectively remove the blurred image, and can be widely used in the field of natural motion-blurred image de-blurring.

Keywords:

Deblurring; Double discriminator; Edge extraction; Generating an antagonistic neural network

1. Introduction

Image blurring is caused by the inability of the photographic equipment to keep relative static with the photographic object. How to remove the blur and obtain a clear image has become one of the important contents of image recognition and detection. Motion image blur can be considered as a clear image convolution on the fuzzy kernel function, coupled with a variety of noise. There are two main categories in the research of image de-blurring: blind de-blurring and non-blind de-blurring. This research mainly involves the field of blindness and blurring.

Blind defuzzification methods can be divided into two classes: estimation of the fuzzy kernel and end-to-end defuzzification of image. References [1] Defuzzification by solving several local fuzzy kernels and fusing the similarity into a global fuzzy kernels；References [2] Estimates fuzzy kernels by adding edge information as constraints, but these methods based on estimated fuzzy kernels are susceptible to noise-induced inaccurate estimates of fuzzy kernels for motion blur, resulting in ineffective de-blurring. To solve these problems, with the rapid development of deep learning, skipping the phase of fuzzy kernel estimation and directly implementing end-to-end image de-blurring has become the mainstream. References [3] Neural network based on antagonism generation and adding sense loss function to end-to-end image de-blurring method, but the noise data is sensitive, the de-blurring effect is poor and artifact is easy to produce. References [4] Generating antagonistic neural networks by adding edge information as auxiliary information and using multiscale networks as edge heuristics of generator network structure, but its training is too complex and its computation is too complex. Therefore, improving the performance of image de-blurring and suppressing artifacts and ringing are the difficulties of current end-to-end de-blurring methods.

Based on the traditional conditions, the fuzzy image is preprocessed to extract the edge of the image, and then the edge of the extracted image is used as auxiliary information for de-blurring processing in the generator. At the same time, we improve the discriminator by using two discriminators to distinguish the de-blurred image and the edge image extracted from the image. Only when the two discriminators are confirmed, the de-blurring effect can be achieved. Because the edge extraction adopts the fusion extraction algorithm, it can extract the significant edge, can reduce the noise interference and suppress the ringing phenomenon, and can reduce the model complexity, so the

double discriminator can guarantee the defuzzification effect very well. The results show that the improved model can achieve a significant de-blurring effect in the case of lower model complexity and higher robustness.

2. Improved modeling

2.1. Model framework

Based on the model of the conditional generated antagonistic neural network, a dual discriminator is introduced to generate the antagonistic neural network, as shown in Figure 1. In the training model, the motion-blurred image Z and the edge image Y_Z obtained through the edge extractor are input into the generator to obtain the restored de-blurred image B. Due to the double discriminator structure of discriminator network, de-blurring image B, clear image X and edge image Y_B and Y_X are sent to real image discriminator and edge image discriminator respectively for training.

The generator and the discriminator compete and play against each other throughout the training model, and the generator is responsible for generating the image while attempting to deceive the discriminator. The discriminator is responsible for distinguishing between the generated image and the clear image. When the discriminator cannot distinguish whether the image is generated for the generator or not, the image generated by the generator has achieved the effect of de-blurring.

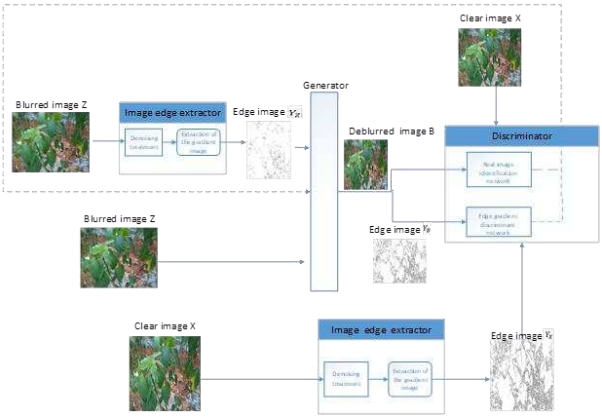


Fig.1 Frame graph of antagonistic neural network based on double discrimination of image edge extraction

2.2. Introduction to Basic Models

2.2.1. Generating an antagonistic neural network

Both the Conditional Generated Confrontation Neural Network and the Edge Based Dual Discriminant Generated Confrontation Neural Network are modified based on the Generated Confrontation Neural Network, which was proposed by Goodfellow [5] and others in 2014 by using the mathematical idea of two-person zero-sum game theory. The whole model is composed of two neural networks: the generator network and the discriminator network. The generator accepts random noise z to generate samples, and the discriminator judges the input samples. The probability of whether the output-input data is "real picture" is trained simultaneously until the discriminator cannot tell whether the sample is "real picture" or not. The objective function is shown in expression (1).

$$\min_G \max_D V(D,G) = E_{x\sim P_{data}(x)}[log\ D(x)] + E_{z\sim P_Z(z)}[log(1-D(G(z)))] \quad (1)$$

Where z is random noise, x is real data, G is generator, D is discriminatory, $\log D(x)$ is discriminator's judgment of real data, and $log(1-D(G(z)))$ is the expression of judgment of generated data. Training maximizes the value of $D(x)$ that is true and minimizes the value of $D(G(z)$ that is true, based on which the Nash equilibrium of the whole game model is achieved by recurring training and optimizing the generation of the network and the discriminant network.

2.2.2. Conditionally generated antagonistic neural network

Conditional Generation Counterwork Neural Network (CGAN) constrains the model and guides data generation by adding an auxiliary information y to both networks of the model based on the original GAN. The model was proposed by Mirza [6] et al. In CGAN, the generator G and the discriminator D are trained at the same time. By adjusting the parameters for the generator G, the objective functions of the conditional GAN are shown in Formula (2), which satisfies the conditions y for both $\min[\log D\,(x|y)]$ and $min[log(1-D(G\,(x|y)))]$.

$$\min_G \max_D V(D,G) = E_{x\sim P_{x(x)}}[log\ D(x|y)] + E_{Z\sim P_Z(Z)}[log(1-D(G(Z|y)))] \quad (2)$$

Where $x\sim P_{x(x)}$、 $Z\sim P_{Z(Z)}$ is the data distribution of clear image and blurred image respectively, E is the mathematical expectation,x is the clear image, Y is the auxiliary information, Z is the blurred image.

2.3. Improved model

The Conditional Generation Counterwork Neural Network Discriminator can get A comprehensive result by inputting the conditional information and the generated picture information into the discriminator at the same time, but this method can't restrict the quality of the generator to be deblurring. In addition to the clear image itself, the edge image of a clear image should also be clear. Therefore, the discriminator is reformed into a double discriminator structure, that is to say, the restored image and the extracted edge image are independently judged, and the image can be deblurred only after both discriminators are recognized. The discriminator and the generator are trained at the same time when the discriminator cannot distinguish the clear image from the generated image, that is, the generator and the discriminator are balanced.

Because of the gradient disappearance and the slow training in the process of calculating the loss function and iterative training, the original CGAN discriminator is modified into two discriminant networks, and the WGAN-GP[7] method is used as the discriminant function. The optimized objective function is shown in formula (3).

$$\min_G \max_D V(D,G) = \max_{D_1}\{E_{x\sim P_{x(x)}}[D(X)] - E_{z\sim P_{z(Z)}}\left[D_1\left(G(Z)\right)\right] - \lambda E_{\tilde{x}\sim P_{\tilde{x}}}\left(\left|\left|\nabla_{\tilde{x}} D_1(\tilde{x}) - 1\right|\right|\right)^2\} + \max_{D_2}\{E_{Y_X\sim P_{Y_{X(Y_X)}}}[D(Y_X)] - E_{Y_Z\sim P_{Y_Z(Y_Z)}}\left[D_2\left(G(Y_Z)\right)\right] - \lambda E_{\widehat{Y_X}\sim P_{\widehat{Y_X}}}(||\nabla_x D_2(x) - 1||)^2\} \quad (3)$$

Where $x\sim P_{x(x)}$, $Y_X\sim P_{Y_X}$ represent the data distribution in the clear image and the corresponding edge image respectively, $z\sim P_{z(Z)}$ 、 $Y_Z\sim P_{Y_Z(Y_Z)}$ represent the data distribution in the blurred image and the corresponding edge image respectively; $\tilde{x}\sim P_{\tilde{x}}$ represents the real image X and a random sample in the connection between the sampled data samples in the generated image B, $\tilde{x} = \left(G(Z)\middle|z\sim P_{Z(Z)}\right)$ in which; $\widehat{Y_X}\sim P_{\widehat{Y_X}}$ represents the real edge image Y_X and a random sample in the connection between the sampled data samples in the generated edge image Y_B, where $\widehat{Y_X} = \left(G(Y_Z)\middle|Y_X\sim P_{Y_X}\right)$; E represents the mathematical expectation, D_1 represents the real image discrimination network, and D_2 represents the edge discrimination network; X and Y_X represent the clear image and its corresponding edge image respectively, and Z and Y_Z represent the blurred image and its corresponding edge image respectively.

2.3.1. The improved edge extraction algorithm

Because the extracted edge image will be used as the auxiliary information to generate the antagonistic neural network, the generator is guided to generate clear images. The effect of image edge extraction will directly affect the quality of the model, so an image extractor is designed to extract image edge. In the process of image edge extraction, image noise will have a great impact on image edge extraction, so in the edge extractor, the image is first denoised by using guided filtering [8]. There are various defects in a single edge extraction operator, for example, Laplace operator[9]and Canny[10] susceptible to picture noise; although the Sobel[11] operator can effectively suppress noise, it is apt to generate false edges； Prewitt operator [12] Edge extraction is less accurate. To extract the prominent edge better, the edge extraction algorithm proposed by the operator in references [2] is adopted. The edge detection algorithm obtains the prominent edge by weighting the four operators of Sobel, Roberts, Prewitt, and Canny. The objective function of the algorithm is as shown in the formulas (4) and (5).

$$E_{con} = \frac{1}{1+e^{-\alpha}} \quad (4)$$

$$\alpha = w_1E_s + w_2E_R + w_3E_P + w_4E_c + w_5 \quad (5)$$

Where E_s, E_R, E_P, and E_c represent Sobel, Roberts, Prewitt, and Canny operators, respectively, and w_5 is the correction term. To reduce the impact of image noise on edge extraction, we use guided filtering to reduce image noise before edge extraction.

2.4. The network structure of the improved model

2.4.1. Generator network architecture

The encoder-decoder network architecture is widely used in the field of computer vision [13-14], and similar architectures are used as the generator infrastructure in the research. The generator takes blurred picture Z and blurred picture edge image Y_Z as input and outputs blurred picture B.

The generator network model is shown in Figure 2. The generator consists of 13 blocks, including two $\frac{1}{2}$ spaced convolution blocks, and nine residual block[15], two deconvolution blocks. Each residual block of the nine residual blocks includes a convolution layer, an Instance normalization layer[16], a Relu activation function layer[17], and Dropout[18] regularization is added after the first convolution layer and the probability value is set to $\frac{1}{2}$. The introduction of a global jump connection enables the generator to learn from the fuzzy image to correct the residuals, which makes the model training faster and the

model generalization ability stronger.

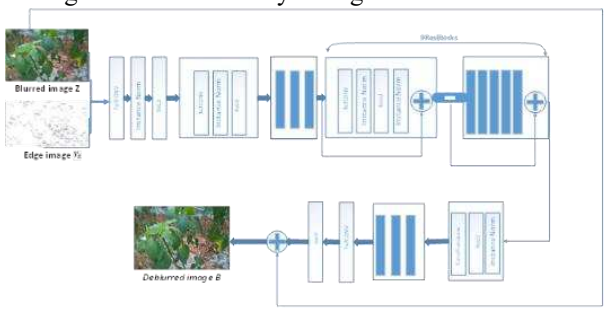


Fig.2 Generator network architecture diagram

2.4.2. Double discriminator network architecture

The double discriminator is composed of real image discriminator and edge discriminator. The two discriminators have the same network structure, but the training samples are different. The training data of the real image discriminator is the clear image corresponding to the blurred image, and the training data of the edge discriminator is the edge gradient image extracted by the edge extractor.

The discriminator network is a Wasserstein GAN[7] (also known as WANP _ GP) with a gradient penalty. Its single discriminator network structure is the same as that of PatchGAN[19]. It consists of five blocks. Each block, except the last, contains a convolution block, an Instance normalization layer, and a LeakyReLU[20] activation layer. The first four blocks get a single discriminator network output by finally connecting a one-dimensional full connection layer and a sigmoid. Finally, the two discriminator network outputs are used as input and connected to a one-dimensional full connection layer and sigmoid to get the final output.

2.5. The loss function of the improved model

2.5.1. Counter loss

Since the WGAN-GP method is used as the discriminant function and two discriminant networks are used, the total countermeasure loss weights of the two discriminators are calculated respectively. The improved countermeasure loss functions are shown in the formulae (6), (7) and (8).

$$L_{GAN} = kL_{D1} + wL_{D2} \tag{6}$$

$$L_{D1} = \sum_{n=1}^{N} -D_{\theta_{D1}}(G_{\theta_G}(B)) \tag{7}$$

$$L_{D2} = \sum_{n=1}^{N} -D_{\theta_{D2}}(G_{\theta_G}(Y_B)) \tag{8}$$

Where $L_{D1}\ and\ L_{D2}$ are the antagonistic loss of real image discrimination network and edge discrimination network respectively, k and w are the weight parameters; B and Y_B represent the restored clear image and the restored edge image respectively.

2.5.2. Perceptual loss

To make the generated image B and the clear image X more similar in content and structure, $L_2\ loss$ is introduced as the content perception loss function to express the difference between the generated image B and the clear image X, as shown in formula (9).

$$L_x = \frac{1}{C_j H_j W_j} \left\| \varphi_j(X) - \varphi_j(B) \right\|_2^2 \tag{9}$$

Where j stands for layer j， $C_j H_j W_j$ represents the size of the Layer j feature map， $\varphi_j(X)$ feature maps representing clear images of layer j， $\varphi_j(B)$ feature mappings representing images generated at layer j， φ_j is derived from the jth convolution block in the pre-trained VGG-19[21] network.

2.5.3. Total loss function

The total loss function is shown in Formula (10), which is a weighted combination of two parts, namely, the counterweight loss and the content perception loss.

$$L = \beta L_{GAN} + \alpha L_x \tag{10}$$

Where L_{GAN} is counter loss, β、α is weighting parameter, L_x loss of content perception.

3. Experimental Design and Result Analysis

3.1. Experimental Design and Evaluation Index

To verify the effectiveness of the algorithm, the improved algorithm is compared with the traditional end-to-end defuzzification model and its simplified model to verify the effectiveness of the defuzzification and the generation of antagonistic neural network structure. In this experiment, peak signal-to-noise ratio (PSNR), structural similarity (SSIM) and average time of deblurring are used as the evaluation indexes. The peak signal-to-noise ratio (PSNR) and structural similarity (SSIM) are calculated as follows (11), (12) and (13).

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\|I(i,j) - K(i,j)\|^2 \quad (11)$$

$$PSNR = 20.log_{10}(\frac{MAX_1}{\sqrt{MSE}}) \quad (12)$$

Where I is clear image, K is deblurred image, m, n for image length and width, MAX_1 is the maximum pixel value for the image.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \quad (13)$$

Where x, y represent deblurred image samples and clear image samples, respectively; μ_x and μ_y represent the average pixels of x and y respectively; σ_x、σ_y represent the pixel standard deviation of x and y respectively, σ_{xy} represents x and y pixel covariance, c_1、c_2 both represent constants.

3.2. Lab Environment and Parameter Settings

All the experiments are based on the Pytorch framework. The hardware configuration is: CPU is Intel i9 9900 k, GPU is NVIDIA GTX 1080TI. The study followed the WGAN-GP training strategy. Using the Adam [22] optimization algorithm, the beta_1=0.92, beta_2=0.999, generator and discriminator cross-training, and first on the discriminator to perform 5 gradient descending steps, and then in the generator once. Initialize Learning Rate to 104 and decay to 10-6 over 600 Periods. Like other CGANs, all models are trained with batch size = 1. Unless otherwise stated, all experiments in this study were trained on the same dataset with the same PC configuration.

3.3. Experimental data set

The study uses the method presented in DeblurGAN [23]. Based on the data released by AI LENGCHANER 2018 Pest and Disease Recognition Challenge, 2000 clear images were blurred by 12 different fuzzy kernels and Gaussian noises with variance 0.0007 and 0.0003 were randomly added to imitate real motion blur, thus a new dataset with 2000 pairs of images was formed.

3.4. Compared with traditional models in image deblurring field

To verify the superiority and effectiveness of the proposed algorithm, the edge heuristic GAN and the deblurGAN method proposed by Orest Kupyn et al., and the edge heuristic GAN proposed by Shuai Zheng et al., are used to eliminate non-uniform blind blur. The three indicators mentioned in 3.1 are used as the evaluation indicators of the experiment. Under the same conditions, the mean values of 30 diagrams were taken as the experimental results by repeating the experiments 30 times on each diagram and testing them independently continuously. Finally, the average of the evaluation index is shown in Table 1, the deblurring time is shown in Table 2, and the deblurring effect is shown in Figure 4.

Table 1 Average of evaluation indicators under the test set

Indicator/method name	Shuai Zheng	Orest Kupyn	Improved algorithm
PSNR（dB）	28.03	27.63	29.99
SSIM	0.845	0.798	0.905

As can be seen from Table 1, the PSNR and SSIM of the improved algorithm are, on average, 6. 9% and 7. 1% higher than those of Shuai Zheng and 8. 5% and 13. 4% higher than those of Orest Kupyn et al. Experimental results show that the de-blurring performance of the proposed algorithm is better than that of other algorithms, which can effectively improve the image de-blurring performance.

Table 2 Average deblurring cost time under the test set

Indicator/method name	Shuai Zheng	Orest Kupyn	Improved algorithm
time（s）	1.2800	1.3360	1.2990

As can be seen from Table 2, the improvement of the algorithm takes 4.3% more time than Shuai Zheng and 2.7% less than Orest Kupyn's method, which shows that the algorithm improves the effect of deblurring, but the time spent does not increase significantly.

Original blurred image	Shuai Zheng	Orest Kupyn	Improved algorithm

Fig.4 Comparison chart of the effect of the deblurring experiment

Experimental results show that the proposed algorithm can remove the motion blur better than other algorithms and restrain the artifact better, and it has better performance in local details than other algorithms.

3.5. Comparison with simplified models

Based on the traditional anti-fuzzy neural network model, the image is pretreated with the guided filter, and then the double discriminator structure is used in the discriminator part to improve the model's ability. To verify the effectiveness of the model, the improved algorithm (Model I) is simplified respectively to form Model II and Model III, where in Model II is the single discriminator model for removing the double discriminatory on the basis of Model I, and Model III is the steps for removing image noise preprocessing on the basis of Model II. The peak signal-to-noise ratio (PSNR) and the structural similarity (SSIM) in 3. 1 are used as evaluation indicators, and the average evaluation indicators are shown in Table 3, and the comparison with the simplified model is shown in Figure 5.

Table 3 Average values of evaluation indicators under test set

Indicator/Model	Model III	Model II	Model I
PSNR	28.99	27.9	29.99
SSIM	0.865	0.803	0.916

As can be seen from Table 3, the improved algorithms PSNR and SSIM are 7% and 14% higher on average than model II, 3.4% and 5.9% higher on average than model III. It shows that the performance of this algorithm is better than other models.

Fig.5 Effect diagram versus simplified model

The experimental results show that the model I is better than the model II in the effect of global de-blurring, and the model I is better than the model III in the effect of local detail than the model three. It is shown that the double discriminator structure and the denoising operation for extracting image edges can effectively improve the image deblurring ability of the model.

4. Conclusion

Aiming at the disadvantages of the GAN network, such as gradient disappearance, gradient explosion, and training instability, this paper proposes a blind image deblurring algorithm based on image edge extraction. Firstly, the image is pretreated by noise reduction. Then, two kinds of discriminators are trained, one is the edge discriminator, the other is the original image discriminator, and the combination of the two discriminators makes the training more stable and simpler, and it is also more advantageous to the constraint generator. The experimental results show that the performance of the improved algorithm is better than other de-blurring algorithms, and it can effectively improve the image de-blurring effect. The next step is to reduce the complexity of the neural network, optimize the model and reduce the dimension of the input data to reduce the complexity of the training greatly.

Acknowledgements

This paper is supported by Chinese National Programs for High Technology Research and Development (No.2006AA01Z428, No.2007AA01Z423).

References

[1] Chen Chunlei, Ye Dongyi, Chen Zhaojiong. Blind Image Deblurring via Multi-local Kernels′Fusion [J]. Acta Photonica Sinica, 2018, 47 (10): 205-215.

[2] Qiu Feng, Hou Fei, Yuan Ye, Wang Wencheng. Blind image deblurring with reinforced use of edges [J]. Journal of Image and Graphics, 2019, 24 (06): 847-858.

[3] Chen Fucheng, Chen Huahua. Image Blind Motion Deblur Algorithm Based on Generative Adversarial Network [J]. Journal of Software, 2019,18 (08): 208-211.

[4] Zheng S, Zhu Z, Cheng J, et al. Edge Heuristic GAN for Non-Uniform Blind Deblurring[J]. IEEE Signal Processing Letters, 2019, 26(10): 1546-1550.

[5] Goodfellow I, Pouget-Abadie J, Mirza M, et al. Generative adversarial nets[C]//Advances in neural information processing systems. 2014: 2672-2680.

[6] Mirza M, Osindero S. Conditional generative adversarial nets[J]. arXiv preprint arXiv:1411.1784, 2014.

[7] Gulrajani I, Ahmed F, Arjovsky M, et al. Improved training of wasserstein gans[C]//Advances in neural information processing systems. 2017: 5767-5777.

[8] Xu Ping, Chen Bingqiang, Xue Lingyun, Zhang Jingcheng, Zhu Lei, Duan Hangbo. A new MNF-BM4D denoising algorithm based on guided filtering for hyperspectral images.[J]. ISA transactions,2019,92.
[9] Mallick, Arijit,Roy, Sourya,Chaudhuri, Sheli Sinha,Roy, Sangita. Optimization of Laplace of Gaussian (LoG) filter for enhanced edge detection: A new approach[P]. Control, Instrumentation, Energy and Communication (CIEC), 2014 International Conference on,2014.
[10] Fengzhi Fu, Chenyuan Wang, Yanlei Li, Hua Fan. An improved adaptive edge detection algorithm based on Canny[P]. Other Conferences,2018.
[11] Ri-Gui Zhou, Da-Qian Liu. Quantum Image Edge Extraction Based on Improved Sobel Operator[J]. International Journal of Theoretical Physics,2019,58(9).
[12] Ri-Gui Zhou, Han Yu, Yu Cheng, Feng-Xin Li. Quantum image edge extraction based on improved Prewitt operator[J]. Quantum Information Processing,2019,18(9).
[13] Su S, Delbracio M, Wang J, et al. Deep video deblurring for hand-held cameras[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2017: 1279-1288.
[14] Xu N, Price B, Cohen S, et al. Deep image matting[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2017: 2970-2979.
[15] He K, Zhang X, Ren S, et al. Deep residual learning for image recognition[C]//Proceedings of the IEEE conference on computer vision and pattern recognition. 2016: 770-778.
[16] Ulyanov D, Vedaldi A, Lempitsky V. Instance normalization: The missing ingredient for fast stylization[J]. arXiv preprint arXiv:1607.08022, 2016.
[17] Nair V, Hinton G E. Rectified linear units improve restricted boltzmann machines[C]//Proceedings of the 27th international conference on machine learning (ICML-10). 2010: 807-814.
[18] Srivastava N, Hinton G, Krizhevsky A, et al. Dropout: a simple way to prevent neural networks from overfitting[J]. The journal of machine learning research, 2014, 15(1): 1929-1958.
[19] Isola P, Zhu J Y, Zhou T, et al. Image-to-image translation with conditional adversarial networks[C]//Proceedings of the IEEE conference on computer vision and pattern recognition. 2017: 1125-1134
[20] Xu B, Wang N, Chen T, et al. Empirical evaluation of rectified activations in convolutional network[J]. arXiv preprint arXiv:1505.00853, 2015.
[21] Simonyan K, Zisserman A. Very deep convolutional networks for large-scale image recognition[J]. arXiv preprint arXiv:1409.1556, 2014.
[22] Kingma D P, Ba J. Adam: A method for stochastic optimization[J]. arXiv preprint arXiv:1412.6980, 2014.
[23] Kupyn O, Budzan V, Mykhailych M, et al. Deblurgan: Blind motion deblurring using conditional adversarial networks[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2018: 8183- 8192.

ZERO-DETERMINANT STRATEGY TO ENHANCE COOPERATION IN INTRUSION DETECTION NETWORKS

HUANG YUANYUAN[1,2], TANG YUAN[1,*], CHEN JIANZHANG[1]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China
[2]Department of Network Engineering, Chengdu University of Information Technology, Chengdu, 610225, China
E-MAIL: iyyhuang@hotmail.com, tangyuanmail@gmail.com, chenyouqing66@gmail.com

Abstract:

With the enlargement of cyberspace scale and development of the network attack technologies, collaborative intrusion detection technology which can effectively improve the security of network systems has been a research focus in recent years. This kind of intrusion detection technology based on distributed computing and cooperation theory is composed of several cooperative intrusion detection systems (IDS). However, individual IDS should be selfish and aim to maximize its own benefits, and might not be effective in cooperative manner in intrusion detection task. This may damage system performance. Therefore, it is of great significance to study the cooperative mechanism among these IDS nodes. In this paper, we simulate the interactions between individual IDS node as a repeated game model by using zero-determinant strategy to deal with the "free riding" behavior, because no matter what the behavior of the adversary is, the game participants can keep the payoffs in the ideal value and achieve the maximum of system payoffs. The numerical results demonstrate that Zero-determinant strategy can enhance the cooperation in intrusion detection networks effectively.

Keywords:

Zero-determinant; Intrusion detection system; Collaborative intrusion detection networks

1. Introduction

In recent years, internet has been widely used and brings great convenience to our work and life. Meanwhile, the information security issues have been a rising threat to our life and work in that the communication infrastructures largely depend on information technology and network engineering [1]. Thus, it is important to establish a safe and reliable environment in cyberspace. As one of the most important countermeasures of the network attack technologies, intrusion detection system (IDS) has been a research focus recently [2]. Specifically, Collaborative Intrusion Detection Networks (CIDNs) were proposed to promote the performance of traditional single intrusion detection system [2]. This kind of Intrusion Detection Networks (IDN) is an overlay network which enables a group of IDSs to cooperate to improve intrusion detection accuracy and detect new attacks. However, the collaboration of IDSs would introduce communication overhead. Since collaboration is based on intrusion information and knowledge exchange, each participant could receive help from others in the network while it has to spend resources to help others in return. However, these subsystems should be selfish and might not be effective in cooperative manner in intrusion detection tasks. This would damage whole system performance. Therefore, it is important to study the cooperative mechanism among IDS nodes of the CIDNs based on game theory. Especially, how to increase willingness of the IDS nodes with low resource capacity to cooperate is a key to solve this problem [2]. Although game theory has been widely used in network security, the application of evolutionary game theory [3] is comparatively new in this research area. In 2009, Xia et al. incorporated evolutionary game theory into the active network defense mechanism [4]. This model describes the detailed interactions between functionally independent parts. In 2013, Ren et al. proposed an evolutionary game model implemented in a distributed manner for collaboration of intrusion detection systems. All these methods try to use game theory-based model to solve the cooperation problem in network security.

In this paper, a Zero-determinant strategy (ZD strategy) based game model to enhance the cooperation among IDS nodes in CIDNs was proposed. As a novel conditional and probability strategy, ZD strategy has been used to content with the "free rider" phenomenon in repeated games. In such

games, the game participator could set the expected payoff of its opponent unilaterally, or set the ratio between the expected payoff of itself and its opponent via ZD strategy, regardless of the opponent's choice [5-7]. We simulate the interaction between the IDS nodes as a repeated game, in which ZD strategy is applied. Therefore, no matter what the adversary's behavior is, the certain IDS node could unilaterally maintain the interests under the circumstance that all the IDS nodes devote themselves to the intrusion detection job, so as to achieve the expected and stable system benefits.

The rest of our paper is organized as follows: section two elaborates the problem and gives description of new game model. Section three proposes a game model using ZD strategy to enhance the cooperation of IDS nodes and analyze the conditions for maximum interests. In section four, the ZD strategy is numerically simulated and the conclusion is explained in the last section.

2. Game model description

Suppose a collaborative intrusion detection networks (CDIN) and all its IDS nodes to form a game system [2]. In the game model, the players are these IDS nodes which can accomplish the intrusion detection tasks. Assume each IDS node can be viewed as an independent intrusion detection system. The interactions between these intrusion detection systems could be defined as "join in the cooperative mechanism of intrusion detection effectively"(*E*) or "not join in cooperative mechanism of intrusion detection"(*N*). Assume each IDS node would reasonably chooses strategies to maximize its own benefit. If all IDS nodes choose to join in the cooperative mechanism of intrusion detection, the benefit of the whole system will be high and the whole cost will be shared. If all IDS nodes do not join in cooperative mechanism of intrusion detection, they will lose a lot. If some IDS nodes choose to join in the cooperative mechanism of intrusion detection while others not, the free-rider phenomenon is serious. For example, the IDS node with high resource capacity may prefer to join in the cooperative mechanism of intrusion detection effectively, while IDS nodes with low resource capacity may prefer to choose the free riding strategy and be reluctant to join in the cooperative mechanism of intrusion detection [2]. Therefore, it is important to enhance the cooperation among the subsystems. In this paper, we adopt the patrol game model of the rich and the poor as metaphor [8]. Assume that the patrol cost is C, the property of the rich is r, and the property of the poor is p. If both the rich and the poor patrol, the cost of patrolling is equally shared; if only one patrols, the cost of patrolling is borne by one person; if neither patrol, the property is stolen and the income is 0. It is easy to get the conclusion that the poor may be more reluctant to patrol. Thus, it is easy to understand that patrol corresponding to accept the intrusion detection task effectively, and refusing to patrol corresponding to not accept the intrusion detect task. Assume that there are two independent IDS nodes, X and Y, and IDS X has higher value(rich) while IDS Y has low value(poor). When two IDS nodes accept the task, each IDS node can solve the task with efforts(*E*) or not(*N*), that is, each IDS node has two strategies in our game mode: *E* and *N*. If both nodes choose strategy *E*, then each IDS node will pay the cost $c/2$; If both IDS nodes choose *N*, then each IDS node will lose all; When one IDS node chooses *N*, another IDS node must pay more. Thus, the payoff matrix between two IDS could be showed as in the table below [9].

Table 1 Payoff matrix of IDS nodes

X \ Y	***E***	***N***
E	$\left(r-\frac{c}{2}, p-\frac{c}{2}\right)$	$(r-c, p)$
N	$(r, p-c)$	$(0,0)$

However, the situation will change if the IDS nodes interact repeatedly in that the IDS node needs to consider the influence of its behavior on the future feedback in repeated games. In 2012, Press et al. had proved that repeated games based on ZD strategy could force a fixed linear relationship between the expected returns of game participant [5]. Therefore, we will apply this strategy in our model to get better overall payoffs in the next section.

3. Game analysis and zero-determinant strategy

According to the payoff matrix in table 1, the game model in our work could be seen as a two-person game with two strategies. In a repeated game model, the player is able to infer the strategy that the opponent should adopt in current round according to the results of previous rounds to a certain extent. Besides, memory-one game is usually adopted in repeated games in that long-term memory doesn't have any advantages compared with short-term memory [6-7]. Thus, the strategies of each IDS node depend on the outcomes of previous round only via memory-one game in our work. According to the choices made by the two IDS nodes in the previous round, the results could be got, $xy \in (EE, EN, NE, EE)$. Correspondingly, the payoff of two IDS nodes could be two vectors, $R_X = \left(r-\frac{c}{2}, r-c, r, 0\right)^T$ and $R_Y = \left(p-\frac{c}{2}, p, p-c, 0\right)^T$. IDS node X's strategy can be expressed in $p = (p_1, p_2, p_3, p_4)$ as the probability

choosing to cooperate in current round according to the outcomes of previous round. IDS node Y's strategy is very similar and could be expressed as $q=(q_1,q_2,q_3,q_4)$. The mixed strategy p or q indicates the cooperation probability corresponding to 4 different cases (*EE,EN,NE,NN*). The strategies chosen by two IDS nodes can be illustrated in table below.

Table 2 Strategies of IDS nodes

X \ Y	***E***	***N***
E	p_iq_i	$p_i(1-q_i)$
N	$(1-p_i)q_i$	$(1-p_i)(1-q_i)$

In Table 2, X represents IDS node X and Y represents IDS node Y in a CDIN, *E* and *N* refer to the strategies used by IDS nodes in previous round, p_iq_i , $p_i(1-q_i)$, $(1-p_i)q_i$ and $(1-p_i)(1-q_i)$ $(i,j\in 1,2,3,4)$ represent the probability choosing strategy $xy\in(EE,EN,NE,NN)$ in current round corresponds to the case of previous step[5-8]. Thus, it is easy to get equation below which represents a Markov transition matrix for rows and columns from previous round to the next round in the order of X.

$$\mathrm{M}=\begin{bmatrix} p_1q_1 & p_1(1-q_1) & (1-p_1)q_1 & (1-p_1)(1-q_1) \\ p_2q_3 & p_2(1-q_3) & (1-p_2)q_3 & (1-p_2)(1-q_3) \\ p_3q_2 & p_3(1-q_2) & (1-p_3)q_2 & (1-p_3)(1-q_2) \\ p_4q_4 & p_4(1-q_4) & (1-p_4)q_4 & (1-p_4)(1-q_4) \end{bmatrix} \tag{1}$$

From equation (1), there is a unit eigenvalue since sum of each row of M is one and $M'=M-I$ is singular. Thus, the stable vector $\mathbf{v}$ of *M* or any vector proportional to it, $\mathbf{v}^TM=\mathbf{v}^T$ will be satisfied, or $\mathbf{v}^TM'=0$.

Moreover, we could get $Adj(M')M'=\det(M')I=0$ via Kramer's law, the $Adj(M')$ refers to adjoint matrix of matrix of M'. Each line of this adjoint matrix is proportional to $\mathbf{v}^T$, therefore,

$$Adj(M')=\begin{bmatrix} d_{11} & d_{21} & d_{31} & d_{41} \\ d_{12} & d_{22} & d_{32} & d_{42} \\ d_{13} & d_{23} & d_{33} & d_{43} \\ d_{14} & d_{24} & d_{34} & d_{44} \end{bmatrix} \tag{2}$$

Among them $d_{ij}=(-1)^{i+j}\det(M'_{ij})$. According to equation (2), we can choose the fourth row of $Adj(M')$, $[v_1,v_2,v_3,v_4]\propto[d_{14},d_{24},d_{34},d_{44},]$ can be obtained ($\mathrm{v}^T=[v_1,v_2,v_3,v_4]$). And if we add 1st column of the matrix M' to 2nd and 3rd columns, the value of the determinant $\det(M'_{ij})$ would not change.

$$\mathbf{M}'=\mathbf{M}-\mathbf{I}$$
$$=\begin{bmatrix} -1+p_1q_1 & p_1(1-q_1) & (1-p_1)q_1 & (1-p_1)(1-q_1) \\ p_2q_3 & p_2(1-q_3)-1 & (1-p_2)q_3 & (1-p_2)(1-q_3) \\ p_3q_2 & p_3(1-q_2) & (1-p_3)q_2-1 & (1-p_3)(1-q_2) \\ p_4q_4 & p_4(1-q_4) & (1-p_4)q_4 & (1-p_4)(1-q_4)-1 \end{bmatrix} \tag{3}$$

For an arbitrary vector $\mathbf{f}=[f_1,f_2,f_3,f_4]^T$, the dot product of the vectors $\mathbf{f}$ and $\mathbf{v}$ could be expressed as below.

$$v\bullet f=v^Tf=[v_1,v_2,v_3,v_4]\begin{bmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \end{bmatrix}$$
$$=\det\begin{bmatrix} -1+p_1q_1 & -1+p_1 & -1+q_1 & f_1 \\ p_2q_3 & -1+p_2 & q_3 & f_2 \\ p_3q_2 & p_3 & -1+q_2 & f_3 \\ p_4q_4 & p_4 & q_4 & f_4 \end{bmatrix}=D(p,q,f) \tag{4}$$

The result of $\mathrm{v}\bullet\mathrm{f}$ can be expressed by a determinant, and 2nd column is $\tilde{\mathrm{p}}=(-1+p_1,-1+p_2,p_3,p_4)$, controlled by IDS node X alone; the 3rd column is $\tilde{\mathrm{q}}=(-1+q_1,q_3,-1+q_2,p_4)$, controlled by IDS node Y solely; The 4th column has only vector $\mathbf{f}$.

Meanwhile, single round payoff vectors of IDS node X and IDS node Y are:

$$\mathrm{R}_X=\left(r-\frac{c}{2},r-c,r,0\right)^T \tag{5}$$

$$\mathrm{R}_Y=\left(p-\frac{c}{2},p,p-c,0\right)^T \tag{6}$$

Thus, the corresponding expected payoff is

$$\begin{cases} w_X=\dfrac{\mathbf{v}\mathrm{R}_X}{\mathbf{v}\cdot\mathbf{1}}=\dfrac{D(\mathbf{p},\mathbf{q},\mathrm{R}_X)}{D(\mathbf{p},\mathbf{q},\mathbf{1})} \\ w_Y=\dfrac{\mathbf{v}\mathrm{R}_Y}{\mathbf{v}\cdot\mathbf{1}}=\dfrac{D(\mathbf{p},\mathbf{q},\mathrm{R}_Y)}{D(\mathbf{p},\mathbf{q},\mathbf{1})} \end{cases} \tag{7}$$

where all components in vector $\mathbf{1}$ are one. The denominator ensures that the sum of all components in vector $\mathbf{v}$ is one, and this is a required condition. The expected payoff w_X and w_Y in (7) depend on the payoff vectors R_X and R_Y linearly. Moreover, it is easy to get that any linear combination of w_X and w_Y would satisfy this relationship, thus equation (8) could be got:

$$\alpha w_X + \beta w_Y + \delta = \frac{D(\mathbf{p},\mathbf{q},a\mathrm{R}_X + \beta \mathrm{R}_Y + \delta \mathbf{1})}{D(\mathbf{p},\mathbf{q},\mathbf{1})} \quad (8)$$

According to the above equation, both IDS node X and IDS node Y have an opportunity to choose a strategy that could make the determinant on the right zero unilaterally. If the strategy chosen by IDS node X satisfy $\tilde{\mathbf{p}} \equiv \alpha \mathbf{R}_X + \beta \mathbf{R}_Y + \delta \mathbf{1}$, or the strategy chosen by IDS node Y satisfy $\tilde{\mathbf{q}} \equiv \alpha \mathbf{R}_X + \beta \mathbf{R}_Y + \delta \mathbf{1}$, the determinant in formula (8) will be zero, and the linear relationship between w_X and w_Y can be expressed below.

$$\alpha w_X + \beta w_Y + \delta = 0 \quad (9)$$

In fact, the above analysis is mainly based on ZD strategy [6-9]. According to equation (9), when IDS node X chooses ZD strategy, no matter what strategy its opponent adopted, the payoffs of IDS node X and IDS node Y are linearly related ($\alpha/\beta \le 0$). IDS node X's strategy $\mathbf{p}$ will meet the equation below.

$$\begin{bmatrix} p_1 - 1 \\ p_2 - 1 \\ p_3 \\ p_4 \end{bmatrix} = \begin{bmatrix} \alpha(r - \frac{c}{2}) + \beta(p - \frac{c}{2}) + \delta \\ \alpha(r-c) + \beta p + \delta \\ \alpha r + \beta(p-c) + \delta \\ \alpha 0 + \beta 0 + \delta] \end{bmatrix} \quad (10)$$

For probability $0 \le p_i \le 1 (i = 1,2,3,4)$, it is easy to obtain the ranges below:

$$\begin{cases} 0 \le \alpha(r - c/2) + \beta(p - c/2) + \delta + 1 \le 1 \\ 0 \le \alpha(r-c) + \beta p + \delta + 1 \le 1 \\ 0 \le \alpha r + \beta(p-c) + \delta \le 1 \\ 0 \le \delta \le 1 \end{cases} \quad (11)$$

Next, we can get the range of parameters α , β and δ by transforming the above formula,

$$\begin{cases} -1 \le \alpha/\beta < 0 \\ \delta \le \min(-\alpha(r - c/2) - \beta(p - c/2), -\alpha(r-c) - \beta p) \\ \delta \ge \max(-\alpha r - \beta(p-c), 0) \end{cases} \quad (12)$$

Based on (11), the IDS node Y's strategy is evolving, and it will try to maximize the payoff of itself. Based on the analysis above, it is easy to get that when IDS node X selects ZD strategy to meet $\alpha w_X + \beta w_Y + \gamma = 0 (\alpha/\beta < 0)$, IDS node Y would like to maximize its payoff ultimate expected.

This paper's purpose is to guide both IDS nodes to participate in intrusion detection tasks effectively. If IDS node X tries to get highest overall payoff, it will choose ZD strategy. IDS node X could set the long-term payoff of IDS node Y at a fixed value unilaterally. If set $\alpha = 0$, IDS node X could choose ZD strategy $\tilde{\mathbf{p}} = \beta \mathbf{R}_Y + \delta \mathbf{1}$ to achieve $\beta w_Y + \delta = 0$, and thus $w_Y = -\delta/\beta$.

$$\begin{cases} p_1 = 1 + \beta(p - \frac{c}{2}) + \delta \\ p_2 = 1 + \beta p + \delta \\ p_3 = \beta(p-c) + \delta \\ p_4 = \delta \end{cases} \quad (13)$$

Substituting $w_Y = -\delta/\beta$ into equation (10), the IDS node X's ZD strategy could be got in equation (14).

$$\begin{cases} p_1 = 1 + \left(1 - \frac{p - \frac{c}{2}}{w_Y}\right)\delta \\ p_2 = 1 + \left(1 - \frac{p}{w_Y}\right)\delta \\ p_3 = \left(1 - \frac{p-c}{w_Y}\right)\delta \\ p_4 = \delta \end{cases} \quad (14)$$

And the two conditions are met:

$$\begin{cases} 0 \le \delta \le min\left(\frac{w_Y}{1 - c/2 - w_Y}, \frac{w_Y}{p - w_Y}\right) \\ max(\frac{-1-\delta}{p - c/2}, \frac{-1-\delta}{p}, \frac{-\delta}{p-c}) \le \beta \le min(\frac{-\delta}{p - c/2}, \frac{-\delta}{p}, \frac{1-\delta}{p-c}) \end{cases} \quad (15)$$

After the transformation, p_1, p_2, p_3, p_4 could be used to express β and δ . Besides, the expected payoff of IDS node Y could be expressed by p_1 and p_4 , that means *EE* and *NN* strategies were used in previous round. The expected payoff can be got in equation (16).

$$w_Y = \frac{p_4\left(p - \frac{c}{2}\right)}{p_4 - p_1 + 1} \quad (16)$$

Thus, when IDS node X chooses the strategy $\tilde{\mathbf{p}} = \beta \mathbf{W}_Y + \delta \mathbf{1}$, it could control IDS node Y's payoff within a certain range. Moreover, IDS node X can control IDS node Y's long-term payoff within the scope $\left[p - c,\ p - \frac{c}{2}\right]$ unilaterally.

According to the above analysis, if IDS node X tries to maximize the overall payoff, ZD strategy would be selected. Meanwhile, IDS node Y can obtain the greatest payoff when both IDS nodes opt to collaborate and the lowest payoff when both IDS nodes opt to betray. Therefore, we can draw a conclusion that ZD strategy could enhance the cooperation

in intrusion detection networks and obtain maximum overall benefits [9-10].

4. Numerical Simulation

To verify the above analysis, a numerical simulation is done by comparing the following strategies: ZD strategy $([1,0.975,0.025,0.05])$, Pavlov $([1,0,0,1])$, tit-for-tat (TFT) $([1,0,1,0])$ and an arbitrary strategy $([0.4,0.3,0.2,0.1])$. We set $r=10$, $p=6$, $c=4$, and suppose X represents the "rich" and Y represents the "poor" in the simulations.

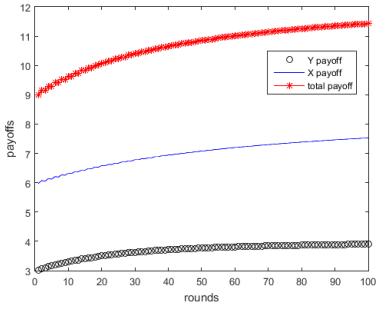


Fig.1 IDS node X selects ZD strategy, IDS node Y selects Pavlov strategy

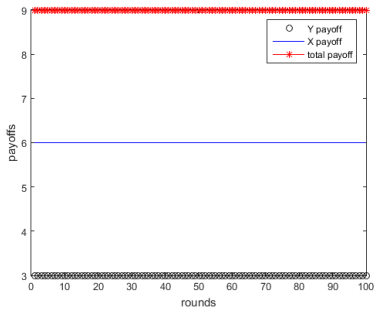


Fig.2 IDS node X selects TFT, IDS node Y selects Pavlov strategy.

As shown in figure 1, IDS node X selects ZD strategy and IDS node Y selects Pavlov strategy, the overall payoff and node payoff could be maintained at a high value stably. In figure 2, when IDS node X selects TFT strategy, IDS node Y selects Pavlov strategy, and the total payoff and the payoff of each IDS node are less than that when IDS node X selects ZD strategy.

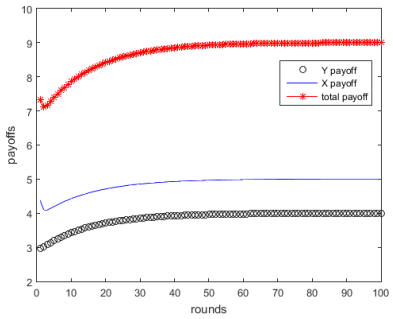


Fig.3 IDS node X selects ZD strategy, IDS node Y selects an arbitrary strategy

As shown in figure 3, when IDS X selects ZD strategy and IDS node Y selects an arbitrary strategy, it shows that the overall payoff and the payoff of each IDS node could be relatively high. Figure 4 illustrates that if IDS node X selects Pavlov strategy and IDS node Y selects an arbitrary strategy, the overall payoff will be lower.

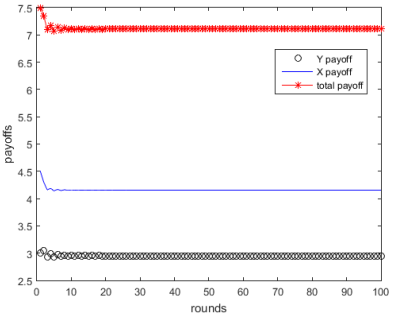


Fig.4 IDS node X selects Pavlov strategy, IDS node Y selects an arbitrary strategy

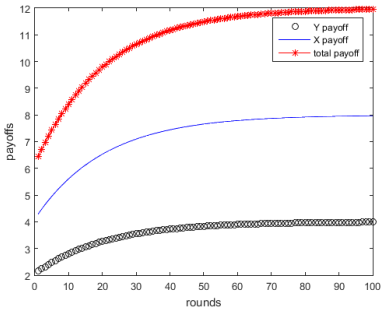


Fig.5 Both IDS node X and IDS node Y select ZD strategy

As shown in figure 5, if both IDS node X and IDS node Y select ZD strategy, the overall payoff reaches the highest value compared with other situations. Thus, this numerical result could demonstrate that zero-determinant strategy could effectively enhance the cooperation in intrusion detection networks.

5. Conclusions

In this paper, Zero-determinant strategy is applied to enhance the cooperation in intrusion detection networks. The IDS node could set payoff of its opponent, without regard for the opponent's behavior, and the greatest overall payoff could be achieved via ZD strategy. Moreover, we simulate and analyze this probability strategy. The experiment shows that ZD strategy could enhance the cooperation phenomenon in collaborative intrusion detection network and maximize the overall benefits.

Acknowledgements

This work was supported by China Postdoctoral Science Foundation under Grant 2018M633354, Sichuan Science and Technology Program under Grant 2018RZ0072 and Foundation of Chengdu University of Information Technology under Grant J201707.

References

[1] Do C. T., Tran N. H., Hong C., et al, "Game theory for cyber security and privacy", ACM Computing Surveys, Vol. 50, No 2. pp.1-37,2017

[2] Fung Carol, "Design and management of collaborative intrusion detection networks", Waterloo, Ontario, Canada, 2013.

[3] M.A.Nowak, "Evolutionary Dynamics", Belknap Press of Harvard University Press, Cambridge, MA, 2006.

[4] Z. Xia. "Research of active network defense mechanism based on evolutionary game theory", Shanghai, China,2009

[5] W. H. Press, F. J. Dyson, "Iterated Prisoner's Dilemma contains strategies that dominate any evolutionary opponent",Proc. Nalt Acad. Sci, Vol. 109, No. 26, pp. 10409-10413, 2012

[6] L.Pan, D. Hao, Z. Rong and T. Zhou, "Zero-determinant strategies in iterated public goods game," Scientific Reports, pp.13096-13096, 2015

[7] J. Chen,Z. Rong, "Zero-determinant strategies for three-player in finitely repeated games", Proceedings of the 37th Chinese Control Conference, Wuhan, China,2018

[8] G. Yao. "Game theory," Nankai University Press, Cambridge, Tianjin, China, 2003.

[9] J. Lu, C. Tang, X. Li, et.al, "Designing socially optimal rating protocols for crowdsourcing contest dilemma", IEEE Transactions on Information Forensics and Security, Vol. 12, No. 6, pp. 1330-1344, 2017

[10] C. Tang, A. Li, X. Li, "When reputation enforces evolutionary cooperation in unreliable MANETs", IEEE transactions on Cybernetics, Vol. 45, No. 10, pp. 2190-2201, 2015

ADDRESS COLLISION ATTACKS ON ECSM PROTECTED BY ADPA

TANG HONG[1], JU TAILIANG[1], LI YAO[1]

[1]School of Information and Communication Engineering, University of Electronic Science and Technology, Chengdu, China
E-MAIL: jutl@uestc.edu.cn

Abstract:

Using the physical characteristics of the encryption device, an attacker can more easily obtain the key, which is called side-channel attack. Common side-channel attacks, such as simple power analysis (SPA) and differential power analysis (DPA), mainly focus on the statistical analysis of the data involved in the encryption algorithm, while there are relatively few studies on the Hamming weight of the addresses. Therefore, a new method of address-based Hamming weight analysis, address collision attack, is proposed in this research. The collision attack method (CA) and support vector machines algorithm (SVM) are used for analysis, meanwhile, the scalar multiplication implemented by protected address-bit DPA (ADPA) can be attack on the ChipWhisperer-Pro CW1200.

Keywords:

Side-channel attack; Address collision attack; Collision attack; Support vector machines; Address-bit DPA;

1. Introduction

With the development of science and technology, the endless information leakage incidents have made people pay more and more attention to information security. Encryption algorithms are the cornerstone of information security, meanwhile, some attack methods have also promoted encryption algorithm.

In 1996, R. Kocher et al. first proposed a side-channel attack method (SCA), and applied this method to RSA encryption and successfully obtained key [1]. Since then, the academic community has started a new wave of research on side-channel attacks. Fan et al. stated that the elliptic curve scalar multiplication (ECSM) implemented by the Double-and-Add algorithm is vulnerable to simple energy analysis attacks (SPA), which greatly threatens the security of the encryption algorithm [6]. Subsequently, the researchers used Double-and-add always resistant against SPA, classic Montgomery ladder and other algorithms to against the SPA attacks [2-3]. However, Hanley et al. proposed that in the calculation process of the classic Montgomery ladder algorithm, there may be data that is not updated and strongly related to the key, which is vulnerable to collision attacks [4]. The frenzy of machine learning algorithms struck, Leo Weissbart and others innovatively applied convolutional neural networks (CNN) to the WolfSSL encryption library based on Curve25519, and used classic template matching, conventional SVM classifiers and CNN classifiers to analysis. It is concluded that the application of CNN for attack has lower signal-to-noise ratio (SNR) requirements for the power trace, and its key recovery accuracy is relatively high [5].

Most of the side-channel attacks are based on the analysis of the relevant data in the encryption algorithm, while the side-channel attacks such as address-bit DPA (ADPA) proposed by Itoh K. et al. have fewer side-channel attacks [7]. Itoh et al. proposed a random address Montgomery ladder algorithm against address-bit DPA attacks. However, there is no side-channel attack method against the improved Montgomery ladder algorithm [8]. The address collision attack is innovatively proposed in the research. Attacker can restore the key of the classic Montgomery ladder algorithm, as well as the Montgomery ladder algorithm proposed by Itoh et al..

2. ECSM algorithm and implementation

2.1. Elliptic curve definition

The elliptic curve cryptography (ECC) was first proposed by Koblitz and Miller in 1985. Its mathematical basis is to use the rational points on the elliptic curve to form the computational difficulty of the elliptic discrete logarithm on the Abel additive group. Compared with the traditional public key encryption algorithm (RSA), the elliptic curve

encryption algorithm has a shorter key length under the same encryption strength.

According to the standard of public key encryption mechanism, there are big differences in the elliptic curve algorithm in the binary domain or prime domain, and the research mainly focuses on the introduction of binary domain. In the binary domain, the non-super-singular elliptic curve equation is defined as formula (1):

$$E(F_{2^m}): y^2 + xy = x^3 + ax^2 + b \quad (1)$$

In the ECC algorithm, all operations are based on the elliptic curve, which provides a security for the algorithm.

2.2. ECSM algorithm introduction

ECSM is also called the key generation algorithm, and this part is the key of the ECC algorithm. If the scalar (that is, the private key) is leaked, the ECC algorithm will no longer have high security. Therefore, a large number of scholars have conducted in-depth research on the security and time complexity of the ECSM algorithm. For example, Itoh et al. proposed a protected address-bit DPA algorithm, as shown in algorithm 1:

Alg.1 Protected Address-Bit DPA Montgomery Ladder algorithm [8]

Input: $P \in E(F_{2^m}), d = (d_{n-1},...,d_1,d_0)_2 \in$

Output: $Q = [d]P$

1) $T[r_{n-1}] = RPC(P)$
2) $T[1-r_{n-1}] = 2T[r_{n-1}]$
3) for i from $n-2$ to 0 do
4) $\quad T[2] = 2T[d_i \oplus r_{i+1}]$ (*1)
5) $\quad T[1] = T[0] + T[1]$
6) $\quad T[0] = T[2-(d_i \oplus r_i)]$
7) $\quad T[1] = T[1+(d_i \oplus r_i)]$ (*2)
8) return $invRPC(T[r_0])$

The implementation of algorithm 1 is consistent with the algorithm proposed by the paper [8], and the operations performed in each round are the same. For functions $RPC()$ and $invRPC()$ introduced in algorithm 1, see the paper [9] for details. In the address-bit DPA analysis, an attacker can get $d_i \oplus r_i = d_j \oplus r_j$, but cannot determine $d_i = d_j$ or not. However, recent studies have found that if an address collision occurs between step (*2) in the previous round and step (*1) in the current round, the relationship between the two adjacent two keys can be analyzed and the complete key can be recovered, that is, the address collision attack. See the next section for detailed attacks.

3. Address collision attack

Given ChipWhisperer-Pro CW1200 side channel analysis package convenience, and the device's stream mode is suitable to ECC algorithm that need to collect large amounts of data, so the research uses it as an experimental platform for attack analysis. At the same time, the platform uses the AVR encryption open source library to implement the ECC algorithm, and calculates the scalar multiplication with algorithm 1. The open source library supports 5 standard curves: secp160r1 (used in study), secp192r1, secp224r1, secp256r1 and secp256k1 can meet research needs.

3.1. Leak model analysis

A power trace is mainly composed of the operation-dependent and data-dependent components. In addition, the trace also includes two parts of noise constant and electronic noise in every power measurement in practice. We refer to the constant power consumption component as P_{const}, the electronic noise as $P_{el.noise}$, the operation-dependent as $P_{op.}$, and the data-dependent as P_{data}.Therefore, the power traces can be modeled as formula (2):

$$P_{total} = P_{op.} + P_{data} + P_{el.noise} + P_{const} \quad (2)$$

In an encrypted device, the load data statement $A = mem\_addr[i]$ can be parsed into two parts: (1) locate the corresponding address; (2) load data from address and save it to A.

This research is interested in part (1) of power consumption information when locating address. Encryption uses the Montgomery ladder algorithm to make the operation-related power consumption of the algorithm constant. Thus, the influence of data and operation can be erased by averaging the power traces, and then the power consumption of part (1) can be obtained. At this point, the power consumption curve can be described as formula (3):

$$P_{total} = P_{local} + P_{const} \quad (3)$$

We refer the information related to the location of the positioning address as P_{local}. This section describes the model of power traces in detail, and the attack will be implemented later.

3.2. Attack analysis

We analyze ECSM implemented by algorithm 1, and the step of research are as follows:

1) Build a data set and collect test data;
2) Build a suitable attack model, train the data set. Then input the test data into the model, and obtain the addresses $T[i]$ and $T[j]$ corresponding to each iteration (*1) and (*2) in algorithm 1;
3) Compare the address $T[i]$ of the previous iteration (*2) with the address $T[j]$ of the current iteration (*1). If $T[i]=T[j]=T[1]$ or $T[i]=T[2]$ and $T[j]=T[0]$ then the key $k_i \oplus k_{i-1}=1$; otherwise $k_i \oplus k_{i-1}=0$. So an attacker can get the information of the adjacent two-digit key.

This research consists of two parts: the profile phase and the attack phase. The profile phase mainly establishes an attack model and verifies it; while in the attack phase, an attack will be carried out with the attack model to recover the complete key.

3.2.1. Profile phase

1) Collect all the power traces related to the memory address and key in algorithm 1, namely $T[0]$, $T[1]$, $T[2]$, and establish the template related address power traces. It can be seen from the description of the above power trace that by averaging the power trace related to addresses with a large amount of random data loaded, the power traces when locating the address can be obtained, and the collected power traces can be verified.

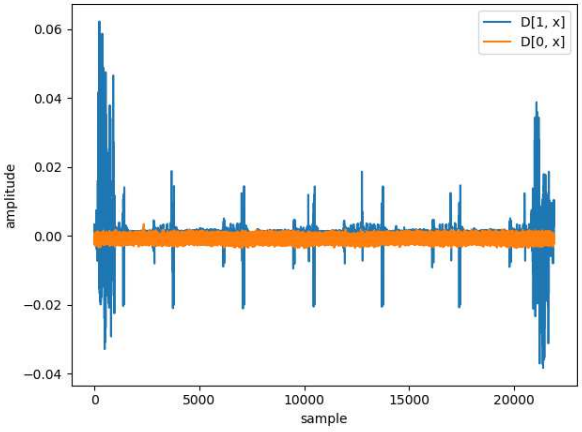


Fig.1 $D[1,x]$ and $D[0,x]$ trace

Set $D[a,b]$ as the difference between the operation address a and the address b , let's Avg_a as the average power trace related to the operation address a , and Avg_b as the trace to address b , then:

$$D[a,b]=Avg_a-Avg_b\begin{cases}=0, & addr_a=addr_b\\ \neq 0, & addr_a\neq addr_b\end{cases} \quad (4)$$

Comparing the trace related to the test address x with the power trace related to address 0 and address 1, shown as Figure 1. It shows that the test address is consistent with address 0 but different from address 1.

In study, 10,000 random data collections are performed for each fixed memory address $T[i](i=0,1,2)$, and each collection has 600 points, then the curve can be described as:

$$Tr_i=\begin{pmatrix} tr_{11} & \cdots & tr_{1n} \\ \vdots & \ddots & \vdots \\ tr_{m1} & \cdots & tr_{mn}\end{pmatrix} \quad (5)$$

Noted that $i=0,1,2$, $m=10000$, $n=600$ and $tr_i=(tr_{i,1},tr_{i,2},\cdots,tr_{i,n})$ as a trace at one round.

And collect a test curve for restoring key. In order to simplify the experiment, only the power traces of 50 rounds of scalar multiplication were collected in the study, and the power traces of each round were obtained by dividing them equally, and using template matching to obtain the power trace corresponding to (*1) and (*2) in algorithm 1 (as shown in Figure 2). Noted as formula (6):

$$test\_tr_i=(pre\_tr_i, post\_tr_i), 0\le i\le 50 \quad (6)$$

In formula (8), pre_tr_i and $post\_tr_i$ respectively represent the power traces corresponding to (*1) and (*2) in algorithm 1.

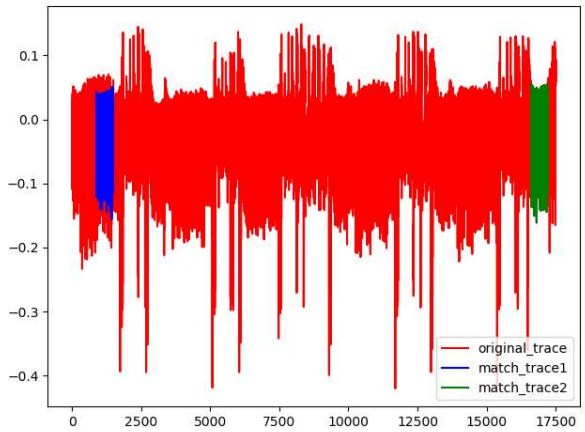


Fig.2 Feature extraction of one iteration

As shown in Figure 2, *original_trace* is the complete primary power trace, *match_trace1* and *match_trace2* are the feature traces obtained by matching pre_tr_i and $post\_tr_i$.

2) Construct the model and determine the power trace related to the address $T[i](i=0,1,2)$. Therefore, the traditional collision attack can be used to obtain its address information; this problem can also be regarded as a classification problem, using common classification algorithms such as support vector machines (SVM) or convolutional neural network (CNN) to achieve. In our study, the traditional collision attack (CA) and SVM were used for analysis and comparison.

Collision attack analysis get the average power trace by averaging the $Tr_i(i=0,1,2)$ corresponding to each address of the power trace, and marks its address as a template for collision analysis.

SVM analysis directly inputs the trace into the built SVM classifier for training. The classifier is implemented using the scikit-learn open source package SVM, and the corresponding parameters are adjusted to obtain a better classification effect.

The research compares the collision attack with the SVM analysis, and analyzes the 50~1200 power traces one by one. The results are shown in Figure 3.

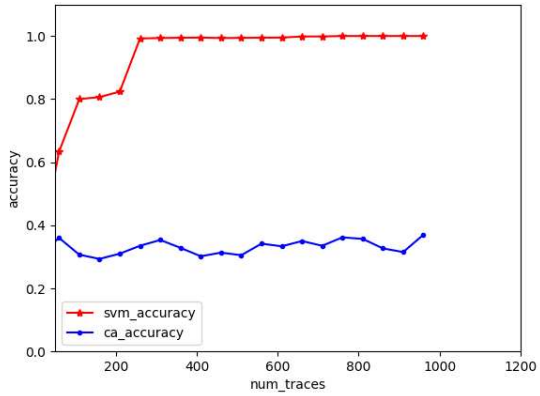


Fig.3 Accuracy comparison between SVM and CA

As shown in Figure 3, SVM analysis can achieve 98% accuracy with about 300 traces, while the accuracy of collision attacks has been low, only about 38%. Therefore, this research directly uses SVM as an attack model for attack analysis.

3.2.2. Attack phase

In the attack phase, each round of trace $test\_tr_i$, $0 \le i \le 50$ is used as the input of the SVM classifier, and the address of step (*1) and (*2) involved in current round of operation can be obtained. Finally, the key can be obtained by parsing the address information. The detailed analysis is shown as Figure 4.

In Figure 4, the detailed analysis of *collision analysis* can get the relationship between adjacent key-bits. Because the value of the highest bit is not clear, two possible key information can be obtained from the key relationship of the adjacent two bits. Finally, the correct key can be obtained by verifying the known base point and public key. At present, the accuracy of key recovery obtained by the address collision analysis used in the research is about 75%.

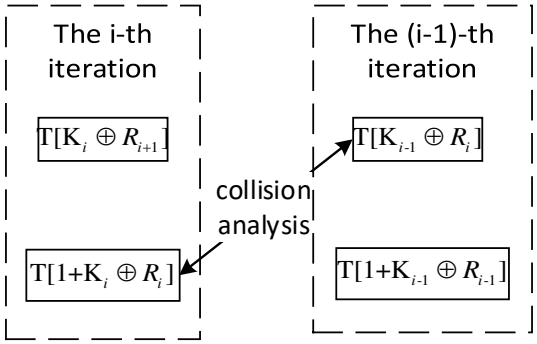


Fig.4 Analysis between two adjacent iterations

3.3. Experimental results

The research uses collision attacks and SVM analysis to compare, and it shows that SVM analysis has more advantages. As the number of power traces used in attacks increases, the accuracy of collision attacks remains at about 38%, while SVM shows an increasing trend, and finally the accuracy is stable at around 98%. There is a certain correlation between the addresses in the power traces, that is, the correlation coefficients of the two are relatively similar. Therefore, it is difficult to perform correct feature analysis only through the Pearson correlation coefficient, the accuracy of collision attacks has always been low. The features of the power trace are not obvious, but the Hamming weight distribution of the address has a certain linear relationship. Thus, in the SVM analysis, the linear kernel function is used to implement the SVM classifier, and about 300 power consumption curves can be used to obtain a higher accuracy, which further proves that the attack model used in our research is more in line with the requirements.

4. Conclusions and future work

There are few side-channel analyses on address information at home and abroad. The research innovatively

proposes an address collision attack, even the Montgomery ladder scalar multiplication with protection will be attacked. Meanwhile, the Montgomery ladder algorithm adds random numbers, but the relevant address information can be obtained through collision-like attacks, so the algorithm has certain defects. The algorithm can be protected by hardware random registers [10].

However, the research also has shortcomings. The accuracy of key recovery is strongly related to the accuracy of determining address information. If there is an error in the determination of the address information, it may have a greater impact on the accuracy of key recovery. Therefore, the key recovery part needs further research, such as adding multiple iterations for cross-validation. At the same time, the model also needs to output the classification probability of each address information. Finally, the Bayesian classifier is used to analyze the final key to improve the accuracy of key recovery.

Acknowledgements

This paper is funded by the Research and Standardization of Key Technologies of IoT Terminal Evaluation Platform (No. 2018YFB2100200).

References

[1] Kocher P., Jaffe J., Jun B. (1999) Differential Power Analysis. In: Wiener M. (eds) Advances in Cryptology — CRYPTO' 99. CRYPTO 1999. Lecture Notes in Computer Science, vol 1666. Springer, Berlin, Heidelberg.

[2] Coron, J.: Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems. In: Ko¸c, C¸ .K., Paar, C. (eds.) CHES 1999. LNCS, vol. 1717, pp. 292–302.Springer, Heidelberg (1999).

[3] Montgomery, P.L.: Speeding the Pollard and elliptic curve methods of factorization. Mathematics of Computation 48(177), 243–264 (1987).

[4] Hanley, N., Kim, H. S., Tunstall, M.: Exploiting collisions in addition chain-based exponentiation algorithms using a single trace. CT-RSA 2015, LNCS 9048, pp. 431–448, Springer, (2015).

[5] Weissbart L., Picek S., Batina L. (2019) One Trace Is All It Takes: Machine Learning-Based Side-Channel Attack on EdDSA. In: Bhasin S., Mendelson A., Nandi M. (eds) Security, Privacy, and Applied Cryptography Engineering. SPACE 2019. Lecture Notes in Computer Science, vol 11947. Springer, Cham.

[6] Fan, J., Guo, X., Mulder, E. D., Schaumont, P., Preneel, B., Verbauwhede, I.: State of the art of secure ECC implementations: A survey on known side-channel attacks and countermeasures. HOST 2010, IEEE, pp. 76-87, (2010).

[7] Itoh K., Izu T., Takenaka M. (2003) Address-Bit Differential Power Analysis of Cryptographic Schemes OK-ECDH and OK-ECDSA. In: Kaliski B.S., Koç .K., Paar C. (eds) Cryptographic Hardware and Embedded Systems - CHES 2002. CHES 2002. Lecture Notes in Computer Science, vol 2523. Springer, Berlin, Heidelberg.

[8] Itoh K., Izu T., Takenaka M. (2003) A Practical Countermeasure against Address-Bit Differential Power Analysis. In: Walter C.D., Koç Ç.K., Paar C. (eds) Cryptographic Hardware and Embedded Systems - CHES 2003. CHES 2003. Lecture Notes in Computer Science, vol 2779. Springer, Berlin, Heidelberg.

[9] Coron, J.: Resistance against differential power analysis for elliptic curve cryptosystem, CHES'99, LNCS 1717, pp.292-302, Springer-Verlag (1990).

[10] May, D., Muller, H.L. and Smart, N.P.: Random Register Renaming to Foil DPA, CHES 2001, LNCS 2162, pp.28–38, Springer-Verlag (2001).

END-TO-END ANDROID MALWARE CLASSIFICATION BASED ON PURE TRAFFIC IMAGES

PENG YUJIE[1], NIU WEINA[1*], ZHANG XIAOSONG[1], ZHOU JIE[1], WU HAO[1], CHEN RUIDONG[1]

[1] School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

[*]Corresponding author, E-MAIL: niuweina1@126.com

Abstract:

Android security accidents frequently occurred in recent years. It has become an urgent need to propose a method for efficiently detecting and classifying Android malware. Many existing machine learning-based methods often require a lot of time for feature engineering, making it time-consuming to classify malware. To accurately and rapidly detect and classify Android malware, this paper proposes an end-to-end Android malware classification model based on traffic analysis and deep learning. The model uses traffic data generated during the Android APP's runtime as input. First, the traffic data will be processed by a third-party traffic removal module based on the idea of clustering to remove impurity traffic that is not conducive to the classification. Then the pure traffic is converted into pure traffic images which can represent traffic characteristics. Finally, a novel convolutional neural network model named 1.5D-CNN is applied to detect and classify malware by classifying these images. The model was trained and tested on a real Android traffic dataset named CICAndMal2017 which contains the traffic data of benign APPs and four types of malware, and it achieved an average accuracy of 98.5%. Compared with traditional machine learning methods, precision and recall both increased by more than 20 percentage points on average.

Keywords:

Android malware classification; Deep learning; Network traffic; End-to-end

1. Introduction

According to a report released by Ericsson [1], the number of smart mobile devices worldwide in 2019 has reached 7.9 billion, and it is estimated that this number will exceed 8.8 billion by 2025. Today, the network traffic generated by mobile devices has approximately accounted for 80% of global Internet traffic.

As the most popular operating system for mobile devices, Android has developed at an unimaginable speed since its inception due to its ease of use, low hardware requirements, and strong scalability, etc. However, while all kinds of Android devices and APPs [2] greatly facilitate people's daily lives, some developers with evil intensions try to develop all kinds of malware for their profit. A report released by Kaspersky Lab [3] shows that in 2019, Kaspersky detected about 3.5 million Android malware installation packages. There are numerous types of Android malware, such as Adware, SMS malware, Scareware, etc. They will seriously infringe the rights of victims once the attack is successful, therefore, the ability to accurately and timely detect malware and classify them is vital to the subsequent handling of the malware.

During the past few years, more and more malware has used advanced code obfuscation and repackaging techniques, making it tough for many traditional malware detection techniques based on signatures and rules to detect them. Finding other effective malware detection methods has become a research hotspot. Since network traffic is an inevitable product which is produced during the attack process of malware and nearly impossible to conceal, it has caught the attention of more and more researchers. Discovering the characteristics of network behavior to detect and classify malware has become an independent research direction.

To establish an effective Android malware classification model with the utilization of network traffic, in this paper, the following main contributions are made:

1) Removing the third-party traffic of malware to obtain pure malicious traffic by applying the idea of clustering, which significantly increases the accuracy of malware classification.

2) Taking advantage of deep learning to autonomously extract the temporal and spatial features from network traffic and train neural network models on them end-to-end. The model receives traffic data files as the input of it with no limitation on the length of input data, and it can detect and classify malware simultaneously.

3) Combining the advantages of the two-dimensional convolution and the one-dimensional convolution, a novel

convolutional neural network (CNN) named 1.5D-CNN is proposed. This new model outperforms the typical 2D-CNN and 1D-CNN in this task.

The rest of this paper is organized as follows. Section 2 discusses the existing Android malware detection methods based on deep learning and network traffic. Section 3 introduces the methodology of the proposed model in detail. Section 4 evaluates the model and reports experimental results. Finally, section 5 concludes the paper.

2. Related work

Almost all Android malware needs to run online to interact with the command and control (C&C) server or to upload and download malicious payloads, which provides a research basis for malware analysis using network traffic characteristics. There have been many studies on the detection of malware and abnormal traffic by using deep learning on traffic data.

In 2017, Wang et al. used a computer vision-based deep learning method to process traffic generated images using CNN in [4] and [5]. In two studies, they respectively used 1D-CNN to detect encrypted VPN traffic and 2D-CNN to classify network traffic, both achieved good effects. In 2018, Huang et al. designed a multitasking detection framework in [6], which could complete the detection of malware, Trojan and encrypted VPN traffic simultaneously through expanding the structure of a typical CNN by adding multiple fully connected layers to it. In 2019, Wang et al. used natural language processing (NLP) methods to process the extracted URL features in [7]. They designed a multi-view neural network to generate multiple "views", and comprehensively analyze all "views" to perform malware detection.

In 2020, Lotfollahi et al. proposed a traffic classification framework called Deep packet in [8]. They applied stacked autoencoder (SAE) and 1D-CNN to detect encrypted VPN traffic and the framework is highly scalable to be used in other tasks related to traffic identification. In the same year, Feng et al. designed an Android malware detection and classification model with a two-layer classification structure in [9]. The first layer of the model extracts some static features of Android APPs like permissions and uses a fully connected network to process these features, while the second layer uses a neural network model named CACNN based on CNN and Autoencoder to process the traffic images. This two-layer model had a good performance in the classification of Android malware.

These studies listed here include the utilization of various deep learning models to detect abnormal or malicious traffic. However, these papers rarely pay attention to the impurities in the traffic, which hinder the detection and classification of malware by neural network models. Therefore, the model proposed in this paper first removes the third-party traffic from the original traffic data and then uses deep learning to process the obtained pure traffic.

3. Methodology

The model proposed in this paper employs a dynamic analysis method based on network traffic features. In the data pre-processing stage, the traffic file in PCAP format is seen as a collection of numerous flows, and the flows belonging to third-party traffic are clustered to be removed from original traffic data to generate pure first-party traffic. Then the pure traffic is split into sessions, and first several bytes of each session is used to generate an image which can represent the characteristics of the traffic in this session. In the deep learning stage, these images are utilized for training a 1.5D-CNN deep learning model to detect and classify Android malware. The overall architecture of the model is shown in Figure 1.

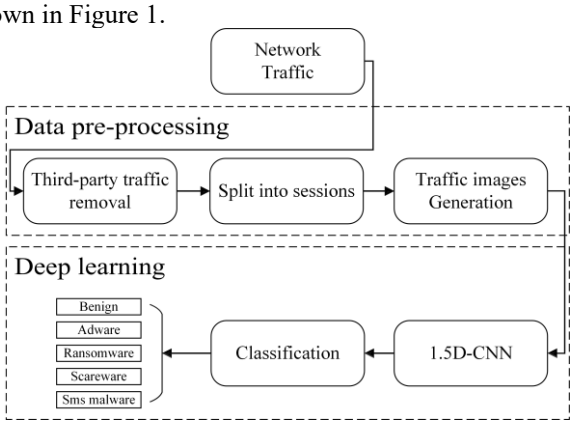


Fig.1 The overall architecture of the proposed model.

3.1. Third-party traffic removal

Generally speaking, two types of traffic are usually generated during the running of malware. The first type is traffic containing malicious behaviors, which are usually generated during the communication with the C&C server or other servers set up by malware developers. This type of traffic can be seen as first-party traffic. Different malware often has unique first-party traffic, which is an essential feature for classifying malware. The second type of traffic is often generated when the APP is using third-party services such as social networking services, Content Delivery Network (CDN) services, and online payment services, etc. Since third-party traffic is shared by much software regardless of their categories, it hinders the detection and classification of malware, therefore, to improve the performance, third-party traffic should be removed from the

original traffic data.

A flow is a collection of packets with the same communication target. For all data packets in the same flow, they have the same source IP, destination IP, source Port, destination Port, and transport layer protocol. It is assumed that the algorithm for removing third-party traffic does not know the label of the PCAP file in advance, the process of removing third-party traffic is shown in Figure 2.

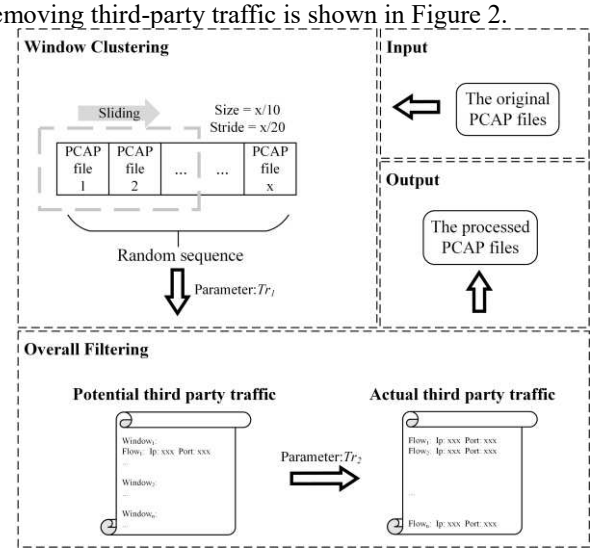


Fig.2 The process of removing third-party traffic

The first stage of the algorithm is called Window Clustering. In this stage, the algorithm employs a sliding window to generate candidates for third-party traffic. The specific method is to arrange all *x* original PCAP files into a sequence in random order and then use a sliding window with a size of *x/10* to process the PCAP files from the beginning to the end in a stride of *x/20*. In each slide of this stage, the flows of *x/10* PCAP files in the window will be clustered according to the threshold Tr_1 to generate potential third-party traffic. The specific generation process is that if there is a flow shared by more than $Tr_1 * x/10$ PCAP files, the traffic of this flow will be seen as potential third-party traffic.

The second stage of the algorithm is called Overall Filtering. Potential third-party traffic generated by each window in the last stage will be filtered from the perspective of all windows according to the threshold Tr_2 to generate actual third-party traffic. The specific method is to first divide all n windows into three window subsets equally from the beginning to the end, and then for the potential third-party traffic generated by all *n* windows in the last stage, if there is some potential third-party traffic generated from more than $Tr_2 * n$ windows and generated at least once in all three window subsets respectively. Then this potential third-party traffic that meets the two above conditions will be considered as actual third-party traffic, and it will be removed from the original traffic.

In this paper, by parameter selection, the threshold Tr_1 is set to 0.4, and the threshold Tr_2 is set to 0.6.

3.2. Traffic images generation

Similar to the definition of the flow, the session is also a collection of a series of specific data packets, more specifically, it is a bidirectional flow which includes two flows of both two communication directions. To process the original traffic data into a data format on which the deep learning models can efficiently and effectively train, the entire traffic data will be segmented into several sessions, i.e., a complete PCAP file will be split into several session PCAP files.

For these session PCAP files, the PCAP header with a length of 24 bytes and the Mac address in each data packet with a length of 12 bytes will be removed. Usually, the length of each session is different, but what needed in deep learning is data with the same format and the same length for training and testing. Therefore, these session PCAP files of different lengths need to be trimmed into an identical length to generate images of the same size.

In this paper, for each session, only the first S_r bytes will be used to generate images, while the rest bytes will be discarded. The S_r is set to 1024 in this paper by parameter selection.

These session PCAP files will be further processed to generate grayscale traffic images. For each trimmed session PCAP file with a size of 1024 bytes, a corresponding image with a size of 32*32 will be obtained. If the size of a session is smaller than 1024 bytes, bytes with the value of 0x00 will be added at the end to fill up the data to 1024 bytes. The specific operation of images generation is to first convert each byte in the PCAP file into a corresponding grayscale pixel according to its value, for example, 0x00 will be converted into a pure black pixel while 0xFF will be converted into a pure white pixel, and then these pixels will be first spliced into rows with a size of 32 from left to right according to the order of the original bytes in the PCAP file, finally, these rows are spliced into an image with a size of 32*32 from top to bottom. Some generated traffic images from an Adware are shown in Figure 3.

Fig.3 Generated traffic images

3.3. 1.5D-CNN

For 2D-CNN, it is adaptive to discover local spatial

features in the traffic images. At the same time, considering that traffic data have a serialized and hierarchical data structure arranged in time, i.e., it is a one-dimensional data stream which is composed of bytes, packets, and sessions. The hierarchical structure of it is similar to the structure of an article which is composed of character, word, and sentence in NLP. Therefore, as 1D-CNN could perform well in NLP tasks, it should also be able to handle traffic data well for they have a lot in common.

Since both 2D-CNN and 1D-CNN can deal with traffic data well, a novel CNN model called 1.5D-CNN is proposed in this paper. It is anticipated that the model can obtain both 2D-CNN's and 1D-CNN's respective advantages and capabilities. The model has both a two-dimensional convolutional layer and a one-dimensional convolutional layer, which first performs two-dimensional convolutions on the traffic images to extract the spatial features of the image, and then performs one-dimensional convolutions on the reshaped feature maps to extract the temporal features. The structure of the proposed 1.5D-CNN is shown in Figure 4, and the main parameters of the proposed 1.5D-CNN are described in Table 1.

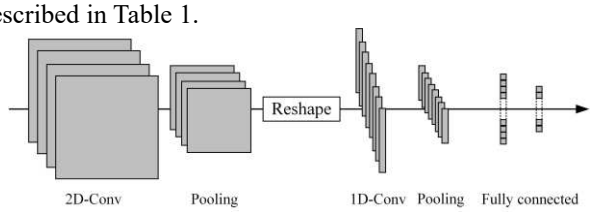


Fig.4 The structure of the proposed 1.5D-CNN

Table 1 The main parameters of the proposed 1.5D-CNN

Layer	Input Shape	Filter	Stride	Output Shape
2D conv+Relu	32*32	5*5	[1,1]	32*32*32
2D max pool	32*32*32	2*2	[2,2]	16*16*32
1D conv+Relu	256*32	25*1	1	256*64
1D max pool	256*64	3*1	3	85*64
full connect	85*64	--	--	1024
full connect	1024	--	--	5
softmax	5	--	--	5

4. Experiment and evaluation

The TensorFlow and Keras are used as deep learning framework which runs on a laptop with 16GB memory and 8 cores CPU. A Nvidia RTX 2060 GPU is utilized as the accelerator.

In the training process, cross-entropy is used as the cost function while Stochastic Gradient Descent (SGD) is used as the optimizer. The training set and test set are divided at a ratio of 9:1, i.e., 90% of the samples in the dataset are used as the training set, while the rest 10% in the dataset are used as the test set.

4.1. Datasets and evaluation metrics

The dataset used in this paper is CICAndMal2017[10] (CICAM), which collects the traffic data of more than 1,700 benign software (BE) obtained from Google Play market and about 400 malware, all traffic data are stored in the format of PCAP file. There are four major types of malware, namely Adware (AD), Ransomware (RA), Scareware (SC) and SMS malware (SMS). This paper randomly selected 110 benign software and all malware in the dataset for experiments. All selected PCAP files were split into sessions as the original session image dataset, called D_S. Then the third-party traffic of all selected PCAP files is removed to get a pure session image dataset, called D_{PS}. The number of samples in each dataset is shown in Table 2.

Table 2 Number of samples

Name	BE	AD	RA	SC	SMS
CICAM	110	91	111	112	109
D_S	72143	193810	192185	218939	133121
D_{PS}	26557	83230	89290	90162	58333

Three commonly used evaluation metrics were used to evaluate models. They are accuracy (A) which measures the overall performance of the classifier, precision (P) and recall (R) which respectively measure the ability of the classifier to find positive samples precisely and comprehensively.

The meaning of each metric can be expressed as the following equations (1).

$$A = \frac{TP+TN}{TP+TN+FP+FN},\ P = \frac{TP}{TP+FP},\ R = \frac{TP}{TP+FN} \quad (1)$$

Where TP is the number of samples which were correctly classified as Y, TN is the number of samples which were correctly classified as Not-Y, FP is the number of samples which were incorrectly classified as Y, and FN is the number of samples which were incorrectly classified as Not-Y. A good classification model should have a high value of all accuracy, precision, and recall.

4.2. Model comparison

To evaluate the performance of 1.5D-CNN, D_{PS} was used as the sample set and four models were trained on the training set respectively, namely 1.5D-CNN, 1D-CNN, 2D-CNN, and LSTM. Then these models were compared by evaluating their performance on the test set. The experimental results, accuracy, precision, and recall of four neural network models on the test set are shown in Table 3.

Table 3 Comparison of four models (%)

	Accuracy	Precision	Recall
1D-CNN	97.9	98.0	97.8
1.5D-CNN	*98.5*	*98.4*	*98.0*
2D-CNN	96.8	96.4	95.4
LSTM	98.2	98.3	98.0

It can be found from the experimental results that for three CNN models, whether in terms of accuracy or other evaluation metrics, the proposed 1.5D-CNN had the best performance, which could classify samples in D_{PS} with an accuracy, a precision, and a recall of 98.5%, 98.4%, 98.0% respectively. It shows that the combination of two different dimensions convolution layers makes 1.5D-CNN have a better ability to extract features from traffic images compared with typical CNN models which only have a single type of convolution layer. At the same time, from the perspective of model complexity, the number of parameters of 1.5D-CNN is about 25% less than that of 1D-CNN, which makes 1.5D-CNN easier and consume fewer resources to be trained. In summary, 1.5D-CNN has the advantages of fewer parameters and the best classification effect among all four deep learning models, hence it is an effective and outstanding CNN model to process network traffic.

4.3. The effectiveness of the third-party traffic removal module

To evaluate the effectiveness of the third-party traffic removal module (TTRM), D_S and D_{PS} were utilized for training models respectively with the same number of iterations. Then the performance of models on two corresponding test sets was evaluated. 1.5D-CNN (1.5D), which had the best performance and 2D-CNN (2D), which had the worst performance in the last experiment were selected as experimental models. The experimental results, the accuracy (A), precision (P), and recall (R) of two CNN models on the test set of D_S and D_{PS} are shown in Table 4.

Table 4 TTRM evaluation (%)

	D_{PS}			D_S		
	A	P	R	A	P	R
1.5D	98.5	98.4	98.0	94.5	94.2	93.1
2D	96.8	96.4	95.4	90.2	89.7	87.2

From the experimental results, it can be found that whether 1.5D-CNN or 2D-CNN was applied as the evaluation model, the effect of malware detection and classification on the test set is greatly improved after removing the third-party traffic. The accuracy of 1.5D-CNN was increased by approximately 4.0 percentage points. For 2D-CNN, which has relatively weak ability to process traffic images, the increase of the accuracy was even more pronounced for it was approximately 6.6 percentage points. In addition to accuracy, for both 1.5D-CNN and 2D-CNN, other metrics also had a significant increase. The experiment results demonstrate the effectiveness of the third-party traffic removal module. Removing the third-party traffic from the original traffic data can significantly improve the effect of detection and classification of malware using neural networks.

4.4. Performance comparison

This paper collected many other studies which used machine learning methods [11-15] and deep learning methods [4][5] to process network traffic, and then evaluated their performance on CICAndMal2017 dataset, thus making performance comparisons. The evaluation results are shown in Table 5 in detail. The 'MC' column indicates whether the method supports multi-classification. If the value in this column is 'N', it means that the method only detects the malware without further classification of which category of the malware is. The 'FE' column indicates whether the method requires feature engineering, i.e., whether it is not an end-to-end method.

Table 5 Performance comparison with other studies

Ref	Pubtime	A	P	R	MC	FE
This paper	N/A	98.5%	98.4%	98.0%	Y	N
[11]	2019	N/A	86.0%	85.0%	Y	Y
[11]	2019	N/A	81.0%	81.0%	Y	Y
[12]	2020	N/A	77.1%	77.1%	Y	Y
[13]	2017	79.1%	83.3%	58.4%	N	Y
[14]	2019	N/A	83.3%	81.0%	Y	Y
[15]	2018	N/A	49.9%	48.5%	Y	Y
[4]	2017	93.9%	93.6%	93.2%	Y	N
[5]	2017	88.2%	88.3%	87.4%	Y	N

Compared with other studies listed in Table 5, the proposed model had increased significantly in both accuracy, precision, and recall. In particular, compared with machine learn-based methods, precision and recall had increased by an average of 21.63 and 26.16 percentage points, respectively. Besides, since the model is end-to-end, no complex feature engineering is required.

5. Conclusion

This paper proposed an end-to-end model that utilizes Android Apps' traffic data and deep learning to detect and classify Android malware. Through the third-party traffic removal module in the model, the impurities in the traffic will be removed, which makes it easier and more accurate

for neural network models to detect and classify Android malware. Pure traffic images, which can effectively represent the malicious network behavior of an Android APP, will be generated from the obtained pure traffic, and then they will be used to train a novel convolutional neural network model named 1.5D-CNN which has both a one-dimensional convolution layer and a two-dimensional convolutional layer. Experimental results showed that the third-party traffic removal module could significantly improve the classification effect and the proposed 1.5D-CNN model outperformed two typical CNN models and one LSTM model in this task. With the help of them, the proposed model achieved a high accuracy of 98.5% on a real Android traffic dataset. Compared with the existing Android malware detection and classification methods using network traffic, the proposed method is not limited by the size of the input, needs no manual feature engineering, and achieves a much better detection and classification performance. In future work, the model will be further optimized and applied in other traffic-related classification tasks.

Acknowledgement

This work was partially supported by the National Key Research and Development Program of China (Grant No. 2016QY13Z2302), the National Natural Science Foundation of China (Grant no. 61902262), the National Defense Innovation Special Zone Program of Science and Technology (Grant no. JG2019055), the Special Central Finance project (Grant Y030202059018060).

References

[1] "(Online) Ericsson Mobility Report 2020". Available: https://www.ericsson.com/en/mobility-report/report.

[2] "(Online) A statistic from a website". Available: https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store.

[3] "(Online) Mobile malware evolution 2019". Available: https://securelist.com/mobile-malware-evolution-2019/96280.

[4] W. Wang, M. Zhu, J. Wang, X. Zeng, and Z. Yang, "End-To-end encrypted traffic classification with one-dimensional convolution neural networks," 2017 IEEE Int. Conf. Intell. Secur. Informatics Secur. Big Data, ISI 2017, pp. 43–48, 2017.

[5] W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, "Malware traffic classification using convolutional neural network for representation learning," Int. Conf. Inf. Netw., pp. 712–717, 2017.

[6] H. Huang, H. Deng, J. Chen, L. Han, and W. Wang, "Automatic multi-task learning system for abnormal network traffic detection," Int. J. Emerg. Technol. Learn., vol. 13, no. 4, pp. 4–20, 2018.

[7] S. Wang et al., "Deep and Broad Learning Based Detection of Android Malware via Network Traffic," 2018 IEEE/ACM 26th Int. Symp. Qual. Serv. IWQoS 2018, 2019.

[8] M. Lotfollahi, M. Jafari Siavoshani, R. Shirali Hossein Zade, and M. Saberian, "Deep packet: a novel approach for encrypted traffic classification using deep learning," Soft Comput., vol. 24, no. 3, pp. 1999–2012, 2020.

[9] J. Feng, L. Shen, Z. Chen, Y. Wang, and H. Li, "A Two-Layer Deep Learning Method for Android Malware Detection Using Network Traffic," IEEE Access, vol. 8, no. July 2013, pp. 125786–125796, 2020.

[10] A. H. Lashkari, A. F. Akadir, H. Gonzalez, K. F. Mbah, and A. A. Ghorbani, "Towards a network-based framework for android malware detection and characterization," Proc. - 2017 15th Annu. Conf. Privacy, Secur. Trust. PST 2017, no. Cic, pp. 233–242, 2018.

[11] R. Chen, Y. L. B, and W. Fang, Android Malware Identification, vol. 1. Springer International Publishing, 2019.

[12] M. Abuthawabeh and K. Mahmoud, "Enhanced android malware detection and family classification, using conversation-level network traffic features," Int. Arab J. Inf. Technol., vol. 17, no. 4 Special Issue, pp. 607–614, 2020.

[13] M. Samara and E. S. M. El-Alfy, "Benchmarking Open-Source Android Malware Detection Tools," 2019 2nd IEEE Middle East North Africa Commun. Conf. MENACOMM 2019, pp. 1–4, 2019.

[14] L. Taheri, A. F. A. Kadir, and A. H. Lashkari, "Extensible android malware detection and family classification using network-flows and API-calls," Proc. - Int. Carnahan Conf. Secur. Technol., vol. 2019-Octob, no. Cic, 2019.

[15] A. H. Lashkari, A. F. A. Kadir, L. Taheri, and A. A. Ghorbani, "Toward Developing a Systematic Approach to Generate Benchmark Android Malware Datasets and Classification," Proc. - Int. Carnahan Conf. Secur. Technol., vol. 2018-Octob, no. Cic, pp. 1–7, 2018.

ANDROID MALWARE CLASSIFICATION APPROACH BASED ON HOST-LEVEL ENCRYPTED TRAFFIC SHAPING

JIE ZHOU[1], WEINA NIU[1*], XIAOSONG ZHANG[1], YUJIE PENG[1], HAO WU[1], TENG HU

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
E-MAIL: vinusniu@gmail.com

Abstract:

With the development of mobile terminals, smartphones have attracted a very huge number of users with their powerful functions. Among them, Android system is famous for its open-source and convenience, which occupies a large market share. But this also leads many attackers to use their malware to gain benefits quickly, which make it necessary to design a practical android malware detection approach. At present, there are not many pieces of research on detecting malware by analyzing Android malicious traffic. This paper examines the characteristics of malicious traffic on the host computer to construct a traffic fingerprint. It combines machine learning algorithms to build a practical detection approach which is also suitable for encrypted traffic. To distinguish similar fuzzy traffic, an additional layer named confusion classifier is added to help further malware classification. This paper uses a real-world dataset called CICAndMal2017 and simulates two classification scenarios: malware binary detection and malware category classification. The experimental results show that the accuracy of the malware binary detection reached 98.8% while the accuracy rate of malware category classification is 95.2%.

Keywords:

Android malware classification; Host-level traffic; Encrypted traffic analysis; Machine learning; Confusion classifier

1. Introduction

With the development of the digital age, smartphones have become an indispensable part of people's daily lives. According to the statistics of Statista, the number of global smartphone users is expected to reach 3.8 billion in 2021 [1]. And in the report of International Data Corporation [2], Android became the most widely used smartphone system in 2019, which occupied 86.7% market share. However, Android has also become the primary target of attackers. According to the report by 360 Mobile Security Research Office [3], there are 1.048 million new mobile malware samples in the first half of 2020, with almost an average of 6 thousand new samples per day.

As user's privacy and experience are greatly threatened by Android malware, we urgently need some effective methods to detect and defend against them. Abnormal network traffic detection [4] is a useful malware detection method that has attracted the attention of more and more researchers in recent years. According to the survey, there are four methods of detecting malware [5]: port-based methods, DPI-based methods, statistics-based methods, and behavior-based methods.

In this paper, we combine methods based on statistics and behavior, use three machine learning methods to classify malware. We have made the following contributions in this paper:

1). We analyze host-level network traffic to detect malware and further identify specific types of them.

2). Our approach weakens the timing features in traffic to improve the accuracy of classification by 5%-10%.

3). We use confusion classifier to deal with data similarities in multiple classifications, which eventually increased the accuracy to 95.2%.

This paper has been organized into five sections. Section 2 describes the related work. Section 3 demonstrates the detection method in detail. Section 4 conducts comparison experiments and analyzes the results. Section 5 provides a summary of the paper.

2. Related work

With the rapid development of malware, a variety of malware variants are emerging, and attackers have made some confusion measures against malware detection methods. There are some researches find that malware traffic fingerprint is an effective detection method. Jiang *et al.* [6] noted that 93% of the Android malware required a network connection to connect with the attacker and receive commands from the C&C server. Besides, Yerima *et al.* [7] analyzed the permissions of 2,000 applications, and more than 93% of malicious applications required network

connectivity. Therefore, more and more researchers are now engaged in the analysis of abnormal network traffic.

In 2011, Iland *et al.* [8] proposed a method of detecting malware and user privacy disclosure by analyzing network traffic. The authors parse HTTP traffic to build a static feature library to detect information leaks and malicious commands. Fakhroddin *et al.* [9] analyzed the network traffic of ransomware in detail, tested the effectiveness of various machine learning models on binary classification and ransomware family classifications. Mohammad *et al.* [10] extracted session-level network traffic characteristics, applied it with a supervised model and conducted experiments in three scenarios. The effect with the same dataset has been significantly improved.

With the spread of HTTPS, more and more researchers have put research centres on the analysis of encrypted traffic. Arora *et al.* [11] proposed an Android malware detection method that does not require the resolution of payloads. They identified seven statistical characteristics for an experiment whose accuracy reached 95%. In addition, Li *et al.* [12] proposed a network traffic monitoring system, which consists of four parts: traffic monitoring, traffic anomaly identification, response processing, and cloud storage. The system parses the packet protocol, extracts the characteristic data (process ID, start time and end time, etc.), and then seed the feature vector to the SVM classifier to find abnormal classes. The experimental results show that the monitoring system is useful in detecting Android malware.

However, there are not many pieces of researches about the malware category classification. Because of this situation, this paper analyzes the differences in data traffic generated by different types of malware, combined with the current machine learning classification algorithm, to find out the specific types of the malware. And to improve the classification accuracy, the confusion classifier is used to assist, the particular approach will be described in section 3.

3. Methodology

This section describes the proposed malware classification approach. The approach mainly analyzes the statistical characteristics and behavioral characteristics of network traffic, combines three machine learning methods for malware classification, and adds a confusion classifier to improve the accuracy of classification. Fig.1 shows the complete structure of the approach, and a detailed description of each part is given below.

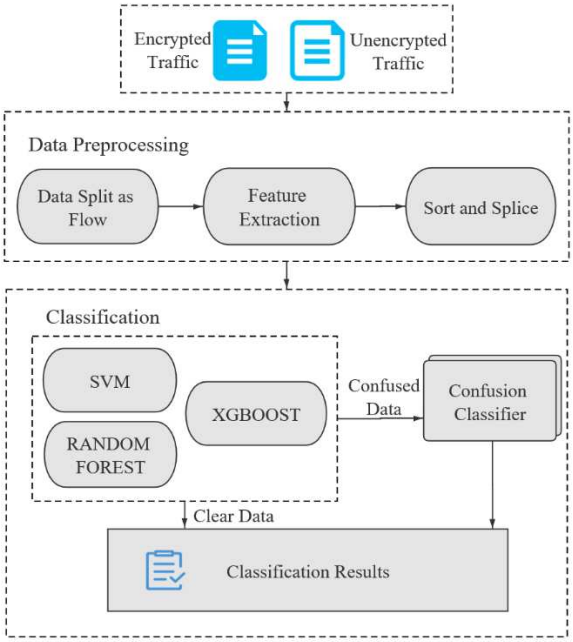


Fig.1 The overall architecture of the approach.

3.1. Traffic preprocessing

Firstly, we divide these complex files into multiple discrete units according to a certain granularity. There are currently five packet segmentation methods [13]: TCP connection, flow, session, service, and host. This paper combines flow and host methods to process PCAP files.

A flow is a collection of data packets with the same five-tuple information including source IP, destination IP, source port, destination port and protocol. However, these malicious behaviors may hide in the usual traffic, so it is unconsidered to directly mark all flows with the same label of the PCAP source file. We can only guarantee that the label of the PCAP source file is reliable, so we merge the feature vector of the flow as the fingerprint of the PCAP file.

3.2. Feature extraction

This paper extracts the initial feature of the flow based on statistics and behavioral methods, including the size of the packet, the number of packets, and the interval between sending packets. Fortunately, the CICFlowMeter [14] tool can help to process the data. The tool divides the PCAP file into units of flows and extracts 76 features for each flow.

All the flows are divided into N groups while the aggregation functions of the feature vectors are calculated in each group. In this paper, maximum, minimum, average and standard deviation is chosen. Then, the feature vector of the

N flow sets are spliced together to obtain a long feature vectors of the entire PCAP file whose dimension is *N**4*76.

Since each malware has different traffic, the time of malicious traffic has a particular impact on the classification. Considering this situation, this paper focuses on whether a certain shaped flow exists, and sorts the value of the same features, which can weaken the influence of the timing features and keep the characteristic information of the flow.

3.3. Machine learning model

We select three machine learning algorithms: SVM, Random Forest, and XGBoost. In the multi-classification experiment, we found that Adware and Scareware are always difficult to distinguish, so we used confusion classifier to help. Firstly, the instances which were classified as Adware and Scareware by the first classifier will be marked as confused. Then confused instances were sent to confusion classifier whose training data is only Adware and Scareware.

4. Experiment and evaluation

All the experiments have been carried out on the Microsoft Windows 10 Professional (64-bit) version with a processor which is i5-7400, 3.00GHz and 16GB of memory. Python 3.7.3 has been chosen for data preprocessing, feature extraction and construction of detection models.

This paper uses the public dataset of the Canadian Institute of Cyber Security which called CICAndMal2017 [15]. CIC was captured in a real mobile phone environment and generated from 2126 Android applications (426 of which were malware and the remaining 1,700 were benign). The PCAP files were divided into five types: Adware, Benign, Ransomware, Scareware, and SMS Malware. Therefore, two classification scenarios were simulated for experiments:

1). Scenario A: divide Android applications into benign and malicious

2). Scenario B: classify Android application software into specific types including Adware, Benign, Ransomware, Scareware and SMS Malware.

Our experiments used 80% of the dataset as the training set and 20% as the test set. And three classifiers: Random Forest, SVM and XGBoost were used for detecting. The experiment adopted the accuracy to evaluate our approach.

First of all, we verified the effectiveness of sorting the same type of features to weaken the effect of segmented position. *N* values were 7, 10, 15, and experiments were conducted in both scenarios. The result is the accuracy of the three machine learning models. As shown in Fig.2, it is not difficult to find that it has a good improvement effect on our detection model to weaken timing features by sorting, and the accuracy rate has increased by 5%-10%.

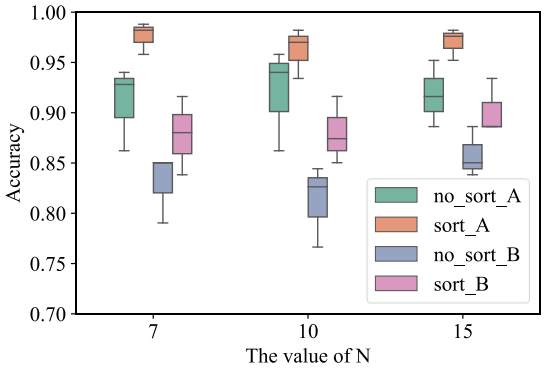


Fig.2 Experiment of weakening timing features.

Then, we change the values of N to find its effect. As shown in Fig.3, the best value is 9 in Scenario A with 98.8% score, and when it turns into Scenario B, the best value is 15.

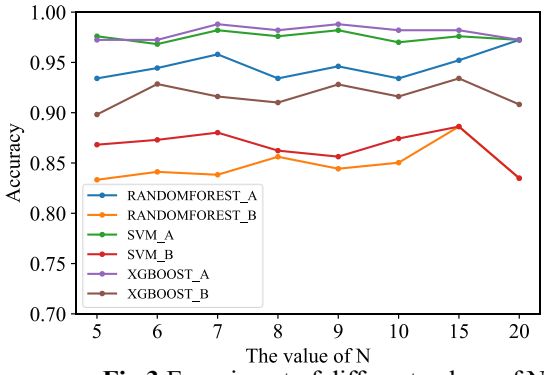


Fig.3 Experiment of different values of N.

The experiment for confusion classifier only works on Scenario B. We choose XGBOOST as the confusion classifier algorithm. The result is shown in Figure 4. Obviously, for three algorithms, the accuracy of confusion classifier is improved. Eventually, our classifier has reached 95.2% accuracy in the work of judging malware categories.

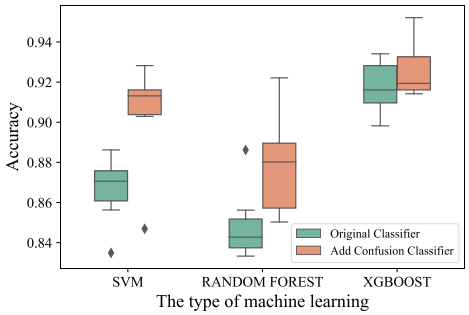


Fig.4 Experiment of confusion classifiers.

Finally, we compared the effect of our approach with CIC [14] and Mohammad [10]. Our model is superior to these two models in both scenario A and scenario B.

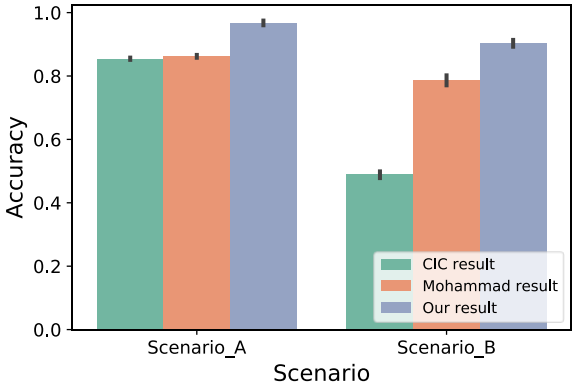


Fig.5 Performance comparison with other studies.

5. Conclusions

This paper proposes an approach to classify malware by analyzing host-level traffic. We use CICAndMal2017 dataset, extract flow characteristics from the flow level, merge the feature vectors to form the fingerprint. Then we use three machine learning algorithms for classification, and design confusion classifier to improve accuracy. Our approach is suitable for encrypted traffic and can effectively detect malware whose accuracy rates reached 98.8% and 95.2% in two scenarios. As part of future work, we plan to combine with other malware detection approaches based on usage permissions and code auditing to obtain a stronger effect.

Acknowledgements

This work was partially supported by the National Key Research and Development Program of China (Grant No. 2016QY13Z2302), the National Natural Science Foundation of China (Grant no. 61902262), the National Defense Innovation Special Zone Program of Science and Technology (Grant no. JG2019055), the Special Central Finance project (Grant Y030202059018060).

References

[1] “(Online) Smartphone Users Report 2020”. Available: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

[2] “(Online) IDC Smartphone Report 2019”. Available: https://www.idc.com/getdoc.jsp?containerId=prUS45487719

[3] “(Online) 360 Smartphone Security 2020”. Available: https://zt.360.cn/1101061855.php?dtid=1101061451&did=610637885

[4] Ahmed, Mohiuddin, Abdun Naser Mahmood, and Jiankun Hu, "A survey of network anomaly detection techniques." Journal of Network and Computer Applications, Vol 60, pp. 19-31, Jan. 2016.

[5] Biersack, Ernst , C. Callegari , and M. Matijasevic . Data Traffic Monitoring and Analysis. Springer Berlin Heidelberg, 2013.

[6] Y. Zhou and X. Jiang, "Dissecting Android Malware: Characterization and Evolution," 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, pp. 95-109, May 2012.

[7] Yerima, Suleiman Y., Sakir Sezer, and Gavin McWilliams. "Analysis of Bayesian classification-based approaches for Android malware detection, " IET Information Security, Vol 8, pp. 25-36, Jan. 2014.

[8] Iland, Danny, Alexander Pucher, and Timm Schauble. "Detecting android malware on network level, " University of California, Santa Barbara, Vol 12, Dec. 2011.

[9] F. Noorbehbahani, F. Rasouli and M. Saberi, "Analysis of Machine Learning Techniques for Ransomware Detection," 2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), Mashhad, Iran, 2019, pp. 128-133, Aug. 2019.

[10] Abuthawabeh M, Mahmoud K, "Enhanced Android Malware Detection and Family Classification, using Conversation-level Network Traffic Features, " International Arab Journal of Information Technology, Vol 17, pp. 607-614, Jul. 2020.

[11] A. Arora, S. Garg and S. K. Peddoju, "Malware Detection Using Network Traffic Analysis in Android Based Mobile Devices," 2014 Eighth International Conference on Next Generation Mobile Apps, Services and Technologies, Oxford, pp. 66-71, Sept. 2014.

[12] J. Li, L. Zhai, X. Zhang and D. Quan, "Research of android malware detection based on network traffic monitoring," 2014 9th IEEE Conference on Industrial Electronics and Applications, Hangzhou, pp. 1739-1744, Jun. 2014.

[13] A. Dainotti, A. Pescape and K. C. Claffy, "Issues and future directions in traffic classification," in IEEE Network, vol. 26, no. 1, pp. 35-40, Jan. 2012.

[14] A. H. Lashkari, A. F. A. Kadir, L. Taheri and A. A. Ghorbani, "Toward Developing a Systematic Approach to Generate Benchmark Android Malware Datasets and Classification," 2018 International Carnahan Conference on Security Technology (ICCST), Montreal, QC, pp. 1-7, Oct. 2018.

MLP-BASED POWER ANALYSIS ATTACKS WITH TWO-POINT JOINT FEATURE SELECTION

LI YAO[1], JU TAILIANG[1], ZHANG CHUNLIAN[1]

[1]School of Information and Communication Engineering, University of Electronic Science and Technology, Chengdu, China
E-MAIL: jutl@uestc.edu.cn

Abstract:

The effective feature selection and classification of power traces in side-channel attacks has been a hot topic of research in recent years. Traditional side-channel attacks, such as simple power analysis attacks and template attacks, require a large number of power traces to break the key, while machine learning algorithms require fewer power traces to successfully recover the key, thus being able to greatly improve the success rate of the attack. Among them, the MLP network proves effective in data classification. Therefore, based on the MLP network, we investigate and propose a power analysis attack method with the feature selection of two joint correlation coefficients. Via comparing the conventional attack methods, the success rate of this attack method is significantly improved.

Keywords:

Side-channel attacks; Machine learning; Two-point joint; Correlation coefficient

1. Introduction

Over the past several decades, cryptography has permeated every aspect of our lives with the rapid development of modern information security technology. Since the publication of cryptographic algorithms, a very large number of attack methods have emerged. In 1996, Kocher first proposed the Side-channel attacks (SCA) method to crack the key of the RSA algorithm through Timing Attacks [1]. In 1999, Kocher et al. Differential Power Analysis (DPA) was proposed and successfully defeated the DES algorithm [2]. In 2002, Chari et al. proposed Template Attacks (TA) and used an example to select keys from an RC4 implementation [3]. In 2004, Brier et al. proposed the Correlation Power Analysis (CPA) attack, which maped the hypothetical power consumption and then found the Pearson correlation coefficient between the actual power value and the hypothetical power consumption value [4]. With the prevalent of machine learning algorithms, the application of related algorithms to template attacks has become the hotspot of current research. In 2011, Hospodar et al. conducted the first in-depth study on the application of machine learning techniques to side-channel attacks by applying the least-squares support vector machine (LS-SVM) to side-channel attacks [5].In 2015, Richard Gilmore et al. proposed a neural network-based side-channel attacks to break the masked AES implementation of DPA contest V4 [6].

However, in both traditional side-channel attacks and machine learning, there exists some limitations therein. In template attack, the inverse of the covariance matrix in the probability density function cannot be performed if the covariance matrix is a singular matrix. While machine learning techniques can bypass the limitations regarding probability density functions, they are prone to overfitting in training, so feature points must be chosen carefully. In this paper, we proposed an optimization method for feature selection by using two-point association with correlation coefficients [7] to attack AES-128 in combination with Multilayer Perceptron (MLP) neural network. The experimental results show that the test accuracy of this feature selection method is much higher than the traditional CPA and SOD methods, and that it can achieve a higher attack success rate with fewer power traces.

This paper is organized as follows: Sect. 2 briefly introduces the principle of side-channel attacks and power leakage model. In Sect. 3, we introduce our network model and feature selection method, followed by the experimental procedure and result analysis. Conclusions of the full text are presented in Sect. 4.

2. Side-channel attacks principle

2.1. Power traces composition

Side-channel attacks use information leaked from hardware during encryption of encrypted devices to obtain keys. The power consumption of a cryptographic device depends on the operations it performs and the data it

processes. For each point in the energy trail, the operation-dependent component is given as P_{op} and the data-dependent component is given as P_{data}. In addition, the actual power consumption also involves electronic noise $P_{el.noise}$, leakage currents and a constant P_{const} caused by operation- and data-independent transistor switching activity. Thus, each point on the power trace can be depicted by using the sum of the operation-dependent component P_{op}, the data-dependent component P_{data}, the electron noise $P_{el.noise}$ and the constant component P_{const}, and the total power P_{total} [8] collected can be expressed as follow:

$$P_{total} = P_{op} + P_{data} + P_{el.noise} + P_{const} \quad (1)$$

In our attack, P_{op} and P_{data} is the power information that we need in relation to the encrypted information.

2.2. Hamming weight model

In power analysis attacks, the number of operations must usually be mapped to an power consumption value when performing power simulation on a cryptographic device. For side-channel attacks, the absolute value of the power consumption is not meaningful in the attack; all that matters is the difference between the power consumptions obtained from multiple simulations. In the Hamming weight model, the Hamming weight $H(x)$ refers to the number of characters in a string x that are non-zero, and the attacker assumes that the power consumption is proportional to the number of bits of the data being processed 1. The Hamming weight model can be described as follows:

$$H(x) = \sum_{i=0}^{n} x_i \quad (2)$$

The power consumption P resulting from a cryptographic chip instruction operation is linearly related to the data it operates on:

$$P = aH(R) + b \quad (3)$$

where P is the sampling power consumption, a is the linear gain between Hamming weight and power consumption, and b is the power consumption of other parts of the register that are not related to the processing data.

3. MLP-based power analysis attacks

3.1. MLP network model

Multi-layer Perception (MLP) is a classical deep learning model where the goal is to approximate a function f^* that, for a classifier $y = f^*(x)$, maps inputs x to a category y. The network defines a mapping $y = f(x;\theta)$ that allows it to get the best approximation of the function by setting the values of the parameters θ. This network plays a significant role in machine learning. For example, convolutional neural network(CNN), which is widely used in image recognition, is a special type of MLP network.

The structure of the multilayer perceptron MLP network is shown in Fig.1 and consists of three main layers, including the input layer, the output layer, and a series of intermediate layers. Each layer consists of one perceptron unit or more, and the weight and bias values of the network are updated iteratively using a gradient learning algorithm. MLP network has two propagation methods, forward propagation and backward propagation.

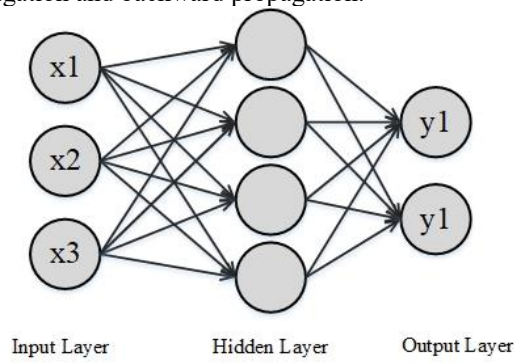


Fig.1 MLP network architecture diagram

MLP based template attacks has obvious advantages compared with traditional CPA, DPA and template attacks. It can also build models in the case of few data samples. The Fig.2 shows the comparison between MLP-based template attacks and traditional template attacks.

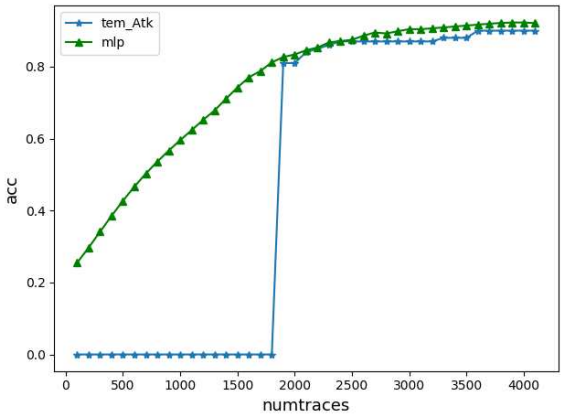


Fig.2 Comparison of the two attacks

As shown in the Fig.2, traditional templates can

successfully attack keys requiring at least 1800 energy traces to execute an attack, while MLP network-based template attacks can be executed with less power traces and higher accuracy.

3.2. Feature selection

In side-channel attacks, not all the points obtained from the power trace sampling are related to the key, but if the features can be selected in advance and then sent to the network for training, the attack effect is often better. Feature selection requires us to determine the location of the power disclosure point and select the features of the leaked power information. In the training stage and testing stage, the selection of the location and number of feature points determines the accuracy of the attack. The traditional CPA method uses the power traces and the Hamming weight model of the selected attack point to analyze the correlation coefficient, and then carry out the attack. The basic equation of the CPA attack is as follows:

$$r_{i,j} = \frac{\sum_{d=1}^{D}\left(h_{d,i}-\bar{h}_i\right)\cdot\left(t_{d,j}-\bar{t}_j\right)}{\sqrt{\sum_{d=1}^{D}\left(h_{d,i}-\bar{h}_i\right)^2\cdot\sum_{d=1}^{D}\left(t_{d,j}-\bar{t}_j\right)^2}} \tag{4}$$

where $r_{i,j}$ is the correlation coefficient between guess key i and sample point j, and $t_{d,j}$ is the measured power consumption of the d_{th} power trace at sample point j; $h_{d,i}$ is the assumed power consumption of guess key i for the d_{th} power trace, for a total of D power traces; $\bar{h}_i$ and $\bar{t}_j$ represent the mean of column h_i of the power consumption value matrix H and column t_j of the measured power trace matrix T, respectively. This is done for all hypothetical keys. If there is a correlation coefficient curve that is significantly higher than the correlation coefficients for the other hypothetical keys at any point in time, then the correct key is the guess key.

Traditionally, correlation coefficient analysis selects features from a single point of attack, but the selected features are often missing, which affects the success rate of the final attack. On the contrary, if two attack points are used for correlation coefficient analysis, the features obtained will be more complete. The common attack points are the input $m_i \oplus d_i$ and the output $S(m_i \oplus d_i)$ of the first round of encryption S-box. In Fig.3, the one-point correlation coefficient analysis is the output of S-box, and the two-point joint correlation coefficient analysis is the input and output of S-box.

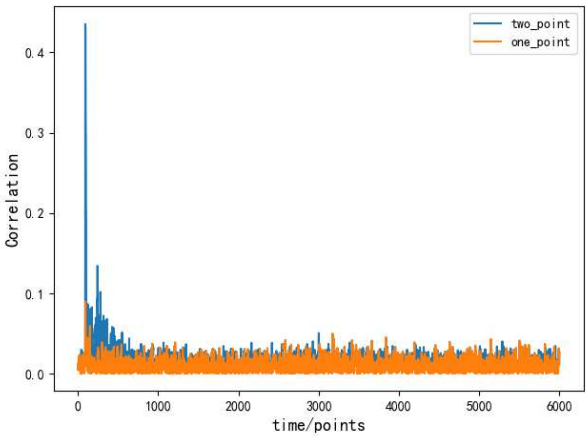


Fig.3 Correlation coefficient comparison

As Fig.3 shows, the correlation of two-point joint is much more obvious. The two-point joint correlation coefficient has relatively larger and more obvious features than the one-point joint correlation coefficient, which is quite suitable for doing feature selection. Therefore, we innovatively proposed a power analysis attack method based on the basis of MLP network with two-point joint correlation coefficient feature selection.

3.3. Attack proposal and implementation

Our experiment uses different feature selection algorithms to analyze the power traces and attack the MLP network, and finally compares the result of different feature selection algorithms on the success rate of key recovery. The experimental attack steps are as follows:

a) Data Acquisition. The data acquisition was done by using the ChipWhisperer platform where the AES-128 cryptographic algorithm was implemented and the power consumption of the cryptographic algorithm while running was collected. The collected power traces are available in the form of training set and test set.

Training set: plaintext random, key random, 4200 power tracks, 6000 points

Test set: plaintext random, fixed key, 100 power tracks, 6000 points

b) Data pre-processing. Since the collected raw data are often too noisy and high dimensional, it is necessary to reduce the dimensionality of the data in advance, PCA, SOD and the two joint correlation coefficient feature selection proposed in this paper are used to pre-process the data, and the number of feature points is set to 650.

c) MLP network model. Since the single power trace is a time series, the number of input nodes in the MLP network is the number of features of the power traces; the hidden

layer adopts the relu activation function; the Hamming weight label value has nine categories, so the output layer is nine nodes, and the Softmax is used as the activation function. The network model has four layers and the network structure table is shown in Table 1.

Table 1 MLP model structure

Genre	Output Size	Activation function	Number of parameters
Input layer	1×650	Relu	-
Dense layer	1×256	Relu	166656
Dropout layer	1×256	Relu	0
Dense layer	1×32	Relu	8224
Dropout layer	1×32	Relu	0
Output layer	1×9	Softmax	297

d) Evaluation index. The main evaluation index in power analysis includes the model's test accuracy, training time and the number of power traces required for key recovery.

3.4. Result evaluation

The experiment is based on the MLP network to model training dataset and test dataset by using different feature selection methods, and the results of the three attacks are shown in Fig.4

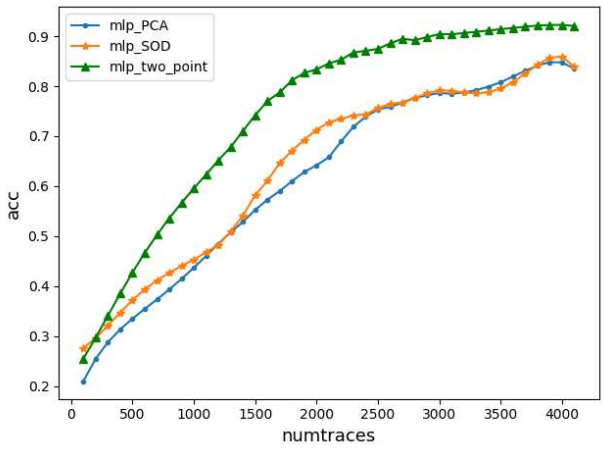


Fig.4 Test Accuracy

As is shown in Fig.4, it's concluded that the attack success rate based on MLP network with two-points joint feature selection is much higher than other two methods, and the curve rises faster, both in the case of fewer power traces.

4. Conclusions

Although traditional side-channel attack is a powerful and feasible method to attack the smart card, it also has some limitations, such as the need for a large number of power traces. Deep learning MLP network can improve some defects of the unified side channel analysis method, but the network is easy to produce the problem of over-fitting in the case of more data eigenvalues. The traditional feature selection algorithms such as PCA and SOD only analyze the energy trace values, but do not use the correlation between the attack point information and the power traces. On the basis of MLP network classifier, we proposed a feature selection method named two-point joint. Our experiments by compared the results of different feature selection methods in power analysis attacks. The results has shown that our feature extraction method is better than the traditional feature extraction method in side-channel attacks.

However, there are still some shortcomings in this paper. For the hamming weight value of 8bit data, the hamming weight value shows a normal distribution, which leads to bare data of some categories in the training process, and the model accuracy converges slowly. In order to solve these problems, we consider to use cross-validation or manually add some category data to improve the success rate of attacks in our future work.

Acknowledgements

This paper is funded by the Research and Standardization of Key Technologies of IoT Terminal Evaluation Platform (No. 2018YFB2100200).

References

[1] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and other systems", in Proc. CRYPTO, LNCS 1109, Springer-Verlag, pp. 104-113,1996.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis", in Proc. Crypto, LNCS 1666, Springer-Verlag, pp. 388-397, 1999.

[3] S. Chari, J.R. Rao, P. Rohatgi, "Template Attacks". in Proc. CHES, vol. LCNS 2523, pp. 13-28, 2002.

[4] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model", CHES 2004, LNCS 3156, pp. 16-29, 2004.

[5] G. Hospodar, B. Gierlichs, and E.D. Mulder, et al, "Machine learning in side-channel analysis: a first study", Journal of Cryptographic Engineering, Vol 1, NO.4, pp. 293-302, 2011.

[6] R. Gilmore, N. Hanley, and M. O'Neill, "Neural network based attack on a masked implementation of AES", in 2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 106–111, May 2015

[7] Du Zhibo，Wu Zhen，and Wang Min，et al, “Multi-Point Joint Power Analysis Attack Against SM4”, Journal of Computer Research and Development, Vol 53, No. 10, pp. 22224-2229,2016.
[8] S. Mangard, E. Oswald E, and T. Popp, Power Analysis Attacks, N.Y. : Springer, New York, 2007

INDUSTRIAL CONTROL SYSTEM INTRUSION DETECTION MODEL BASED ON LSTM & ATTACK TREE

FAN XINGJIE[1], WAN GUOGEN[1*], ZHANG SHIBIN[1], CHEN HAO[1]

[1]School of Cybersecurity, Chengdu University of Information Technology, Chengdu 610225, China
E-MAIL: z1ng3r22@qq.com

Abstract:

With the rapid development of the Industrial Internet, the network security risks faced by industrial control systems (ICSs) are becoming more and more intense. How to do a good job in the security protection of industrial control systems is extremely urgent. For traditional network security, industrial control systems have some unique characteristics, which results in traditional intrusion detection systems that cannot be directly reused on it. Aiming at the industrial control system, this paper constructs all attack paths from the hacker's perspective through the attack tree model, and uses the LSTM algorithm to identify and classify the attack behavior, and then further classify the attack event by extracting atomic actions. Finally, through the constructed attack tree model, the results are reversed and predicted. The results show that the model has a good effect on attack recognition, and can effectively analyze the hacker attack path and predict the next attack target.

Keywords:

ICS; IDS; Attack tree; LSTM

1. Introduction

With the launch of the German "Industry 4.0" [1], the US "re-industrialization" and other national strategies. Meanwhile, Cloud computing, big data, artificial intelligence, Internet of Things and other new-generation information technologies and manufacturing technologies, are accelerating the integration. As a result of the integration of global industrial systems with advanced computing, analysis, sensing technologies and Internet connections, the industrial control system is composed of the original closed and independent move towards openness, from stand-alone to interconnection, and from automation to intelligence. While industrial enterprises have gained great development potential, there are also a large number of potential safety hazards.

Today, industrial control systems are an important part of the country's critical infrastructure. And different from traditional IT systems, once an industrial control system is attacked by a network, it will cause significant property losses, casualties and other unexpected catastrophic consequences. In October 2010, a worm named Worm.Win32. Stuxnet [2] swept the industry, affecting the normal operation of many companies around the world in a short period of time, and it had even caused a delay in generating electricity at Bushehr nuclear plant in Iran. In March 2019, Venezuelan largest power facility, the Guri Dam [3], was attacked. As a result, Venezuelan power system was paralyzed. Caracas, the capital of Venezuela, fell into a power outage at 16:50 p.m., causing thousands of houses to have power and water cuts, subways out of service, and communication services unavailable. It took a week for the Venezuelan government to restore the complete power system.

There are various types of security risks and threats facing the Industrial Internet, including the vulnerability of industrial control system itself, the traditional network attack method, and the attack against the vulnerability of industrial control proprietary protocol. Nowadays, intrusion detection system (IDS) is the main research direction for the discovery of Industrial Internet threat behavior. Marton [4] extracted generator and other operating data and some relative data, including rotor speed, gearbox temperature, generator power, temperature difference between generator and surrounding environment, and environmental temperature difference between generator and engine compartment. The analysis method finds the attributes that best represent the system state in the original data set, and then uses the least square method to predict the system state and detect abnormal behavior. Caselli [5] extracted system status and communication protocol as features, including network communication type, IP address, MAC address, port number, MODUBS function code, time stamp, events in the system, etc., and established event sequence based on the above features Model, and use hidden Markov model to judge abnormality. Vollmer [6] and others applied a genetic algorithm such as multiple emotions to automatically extract the rules of abnormal behavior, and can establish the rules of known intrusive behavior.

At present, the research direction of intrusion detection systems for the Industrial Internet is mainly in the application and improvement of algorithms, the selection and optimization of features. This article starts with the characteristics and logical structure of an industrial control system, and constructs a set of

intrusion detection models with predictive capabilities for industrial control systems.

The model has three stages:

- Attack tree construction: According to the structure and logic of the industrial control system, the attack tree is constructed from the hacker's perspective to ensure that all attack paths are covered as much as possible;
- Attack recognition and detection: Through the trained LSTM model, the attack is identified and classified into several basic attack events. At the same time, by extracting atomic actions, they are further classified into the leaf nodes of the constructed attack tree model;
- Attack prediction: By identifying hacker attack methods and using the constructed attack tree model, infer the attack effect or the next stage of attack target.

2. Features and characteristics

Through a lot of analysis and statistics, it is found that attacks against the industrial Internet often have the following characteristics:

- Multi-step behavior, that is, a threatening behavior often contains multiple steps. For example, the attacker scans, detects, exploits, continues to infiltrate and maintains permissions on peripheral management system servers, and finally attacks industrial control equipment through lateral movement.
- Multi-layer classification. Attacks in ICS can be divided into three categories according to the network deployment level:

1) **Monitoring Network Attack**. This part of the attack source mainly comes from external or internal cyberspace. For example, a hack attacks the external network system, enters the internal network, and then attacks some engineering station/operation station machines through lateral penetration to achieve control purposes. Or use man-in-the-middle attacks to tamper with data and destroy its integrity. This is consistent with traditional hacking techniques and can be directly applied to traditional IDS systems.
2) **System Attack.** This part of the attack is mainly injected into industrial control equipment through some illegal commands.
3) **Process Attack.** This part is mainly because some commands are standardized, but violate the production logic of the entire system, for example, the heat pump and the condenser must be turned on at the same time.

- The time span is long, that is, there may be a long time interval between multiple steps included in the same threat behavior. It can be seen that most of the current attacks on industrial control systems have turned into slow penetration attacks.

For each step of the threat behavior, we can call it a basic attack event. Through the comprehensive analysis of natural gas pipeline control system data set [7] and KDD 99 [8] data set. The common basic attacks in the Industrial Internet can be divided into the following categories.

Table 1 Basic attacks

Basic attacks	Attack types	Description
Normal	/	Normal requests.
Recon	Reconnaissance	Scanning behaviors.
DoS	Dential of Service	Attackers usually target communication links and system programs, sending large amounts of useless data to the target network, disrupting the normal operation of the system, and trying to exhaust resources.
MSCI (Malicious state command injection)	Command Injection [9]	The attacker changes the behavior of the system by injecting wrong control and configuration commands. The potential effects of malicious command injection include loss of process control, equipment communication interruption, unauthorized modification of configuration and set values.
MPCI (Malicious parameter command injection)		
MFCI (Malicious function code command injection)		
NMRI (Naive malicious response injection)	Response Injection	The response injection attack will change the response packet from the server to the client and provide incorrect system status information. NMRI attacks inject or modify response packets in the network; CMRI attacks usually disguise the feedback from
CMRI (Complex malicious response injection)		

		physical devices.
U2R (User to Root)	Exploit	Attackers obtain certain system permissions through such attacks.
R2L (Remote to Login)		
C&C (Command and Control)		

Each basic attack is completed by a combination of one or more atomic actions (AT) [10]. We can understand the atomic action as every network or command request. For example, in an attack on the surveillance network, if there are "frequent login requests in a short period of time", the basic attack event of "password blasting" can be deduced; and usually for system attacks and process attacks, AT may only one or more continuous multi-operation instruction requests. Generally speaking, the combined atomic actions also have a certain timing.

3. Model

According to the characteristics of industrial Internet attacks, we first adopt the method of expert evaluation to structure the entire network structure into layers. At the same time, the attack route is constructed with the attack tree model. However, ICS data has the characteristics of massive and high latitude, and at the same time addresses the problem of long time intervals for APT attacks. Therefore, the LSTM algorithm is selected for the classification of basic attack events. According to the basic attack method of classification, we then use the attack tree model to predict the hacker's attack.

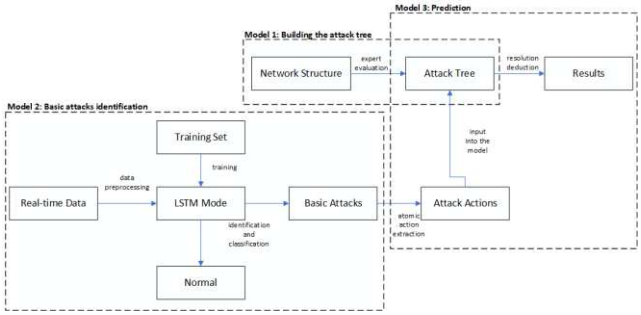


Fig.1 Flow chart of the model

3.1. Attack tree

The attack tree model is a method proposed by Schneider [11] in 1999 to describe multiple attacks that the system may be subjected to. It uses a tree structure to represent the dependency between attack behaviors and steps, and displays the attack process against the target in the form of a graph. In any attack tree, the top of the tree, also known as the root node (Goal, G), represents the final attack even; the middle node (Middle, M) can represent the target at each stage; and the leaf node represents the hacker attack action (Action, A) or attack precondition (Condition, C).

In order to achieve the stage/final goal, there are three causal relationships between each attack event:

- **OR**: Indicates that any child node satisfaction can lead to the realization of the parent node.
- **AND:** It means that the parent node can only be realized if all child nodes are satisfied.
- **SAND:** Indicates that all child nodes need to be satisfied in order to cause the parent node to achieve.

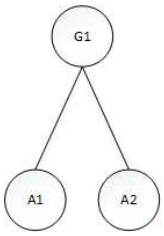


Fig.2 OR tree

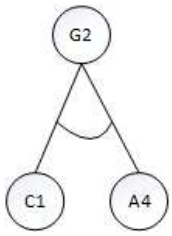


Fig.3 AND tree

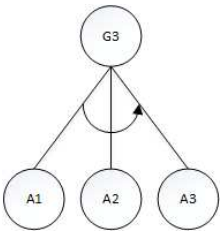


Fig.4 SAND tree

The construction of the attack tree is from top to bottom, and according to the attack tree we have constructed, we can use the resolution method to derive the result from the process in reverse. Then, we can express the above picture by the formula:

- **OR tree:**

$$A1 \vee A2 \rightarrow G1 \tag{1}$$

- **AND tree:**

$$C1 \wedge A4 \rightarrow G2 \tag{2}$$

- **SAND tree:**

$$\neg A1 \rightarrow \neg A2 \tag{3}$$

$$\neg A2 \rightarrow \neg A3 \tag{4}$$

$$A1 \wedge A2 \wedge A3 \rightarrow G3 \tag{5}$$

3.2. LSTM

LSTM, Long Short-Term Memory [12], is a special RNN network. It is proposed to solve the problem of gradient disappearance and gradient explosion of RNN. Simply put, if the time series is too long, the RNN will forget. In order to solve this problem, LSTM introduces a concept: important remember, irrelevant forget. It is realized by three gates. Among them, cell state means "long memory" and hidden state means "short memory". The industrial control system itself has a large amount of network data, and APT attacks also have the characteristic of long-time interval.

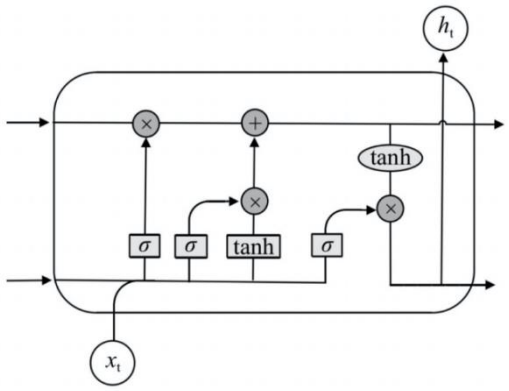


Fig.5 LSTM cell structure

1) **Forget Gate.** Determine what information we need to discard from the previous cell state. This uses the Sigmoid function to put the value between 0 and 1. "1" means completely reserved, "0" means completely discarded, the formula is expressed as:

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f) \quad (6)$$

2) Input Gate. Used to determine what new information needs to be kept in the state of the cell, this is divided into two parts. First, the Sigmoid function determines which values we will update. Next, use the tanh layer to create candidate cell states. The formula is expressed as:

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \quad (7)$$

$$\tilde{C}_t = \tanh W_i \cdot ([h_{t-1}, x_t] + b_c) \quad (8)$$

Next, we should update the value:

$$C_t = f_t * C_{t-1} + i_t * \tilde{C}_t \quad (9)$$

3) Output Gate. It is used to determine what value we need to output, which is determined based on the cell state, expressed as a formula:

$$O_t = \sigma W_o \cdot [h_{t-1}, x_t] + b_o \quad (10)$$

$$h_t = o_t * \sigma \tanh(C_t) \quad (11)$$

3.3. Atomic action extraction

After classifying the basic attack events through LSTM, we extract the corresponding atomic actions to further classify the hacker attack methods. For example, for a drainage system, the attacker forced to open the water inlet valve z1, and we identified it as an MSCI attack through the attack recognition classification. At the same time, our atomic action extraction can extract the target executor and the executor execution action (0 means **OFF**, 1 means **ON**) to form **{MSCI, z1, 0}**, which can be further classified.

4. Experiment

This paper uses SWaT [13] for simulation experiment. The SWaT is a miniature sewage treatment system, which contains six sub-processes, controlled by a group of Allen-Bralley PLCs, and the running status of the PLC is monitored by the SCADA system.

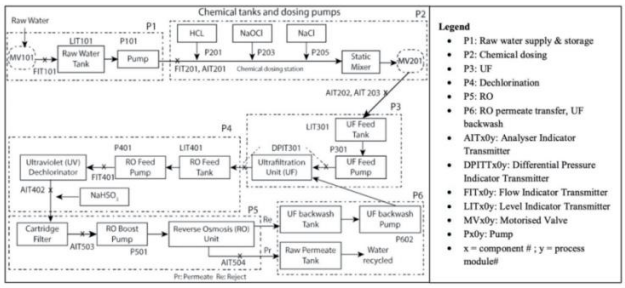


Fig.6 SWaT's six-stage processes

4.1. Building the attack tree

The structure of the P1 module is shown in Figure.6. MV101 is raw water inlet on/off valve; FIT101, LIT101, and FIT201 are sensors for inlet pipe, sewage tank, and outlet pipe respectively; P101, P102(standby) are outlet pumps.

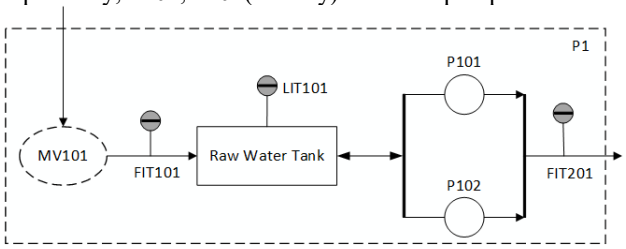


Fig.7 Structure diagram of P1 module in SWaT

We tried to build an attack tree model for the Raw Water Tank overflow in the P1 module.

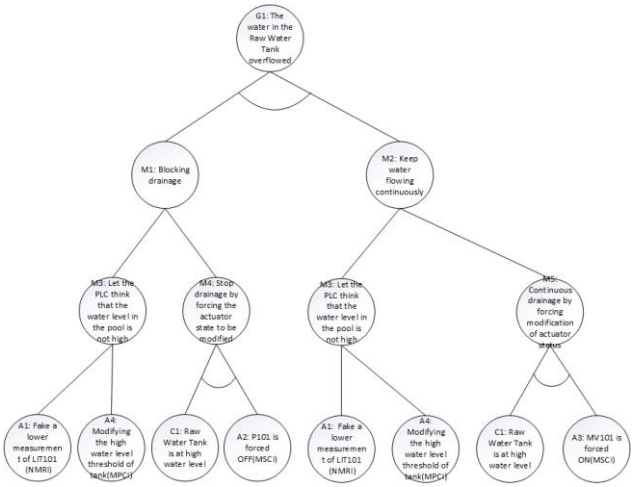


Fig.8 P1 module sewage pond overflow attack tree

It is expressed in mathematical form as:

$$A1 \vee A4 \rightarrow M3 \quad (12)$$

$$A2 \wedge C1 \rightarrow M4 \quad (13)$$

$$A3 \vee C1 \rightarrow M5 \quad (14)$$

$$M3 \vee M4 \rightarrow M1 \quad (15)$$

$$M3 \vee M5 \rightarrow M2 \quad (16)$$

$$M1 \wedge M2 \rightarrow G1 \quad (17)$$

4.2. Basic attacks identification

Through the comparison of several algorithms, we find that LSTM has a good result in the classification of industrial control system attacks.

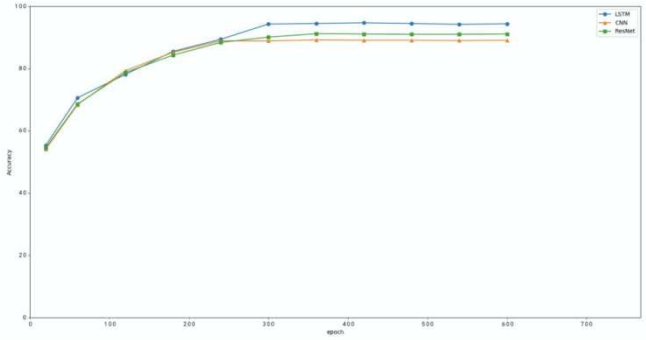


Fig.9 Comparison with other algorithms

We train the LSTM model, and finally select the number of hidden layers (H) to be 50, and the learning rate (r) is 0.1, and relatively good results can be obtained.

Table 2 Effect of different parameters

Parameter	Accuracy /%	Training time /s
H=20, r=0.05	89.2	14.72
H=20, r=0.1	90.4	15.63
H=50, r=0.05	93.6	18.14
H=50, r=0.1	95.4	20.02
H=80, r=0.05	93.4	24.15
H =80, r=0.1	93.2	23.61

According to the 10 attack methods on P1 provided by the test bed, 9 attacks were successfully identified as basic attack and classified. And by extracting atomic actions, continue to be classified as: **A1{x6, x7}**, **A2{x4, x8}**, **A3{x1, x7}**, **A4{null}**. For the 9 types of attacks that were successfully identified, a 100% fine classification was achieved.

4.3. Prediction

According to the attack tree model, we can successfully predict the consequences of our attack. For example, when A1 occurs, it can be concluded from expressions (12), (15), (16), (17) that G1 must occur.

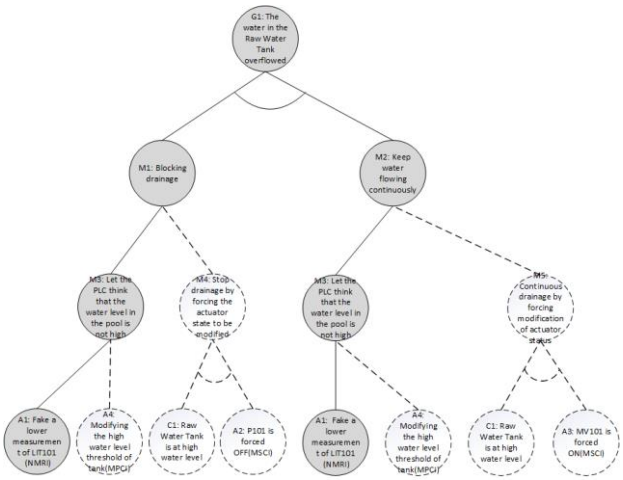


Fig.10 Attack path when A1 occurs

5. Conclusions

This article mainly builds an attack tree model and first simulates the construction of a complete hacker attack route. At the same time, the basic attack event classification is carried out through the LSTM algorithm. Then by extracting the atomic actions, the attacks continue to be classified into the attack tree corresponding to the hacker attack methods. Finally, through the inference of the attack tree model, the hacker's attack target and attack effect are predicted. Through the experiment and evaluation of SWaT data set, the results prove that the

recognition rate and prediction effect of this model are relatively excellent.

References

[1] Lee, J., Bagheri, B. , & Kao, H. A. . (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18-23.

[2] Karnouskos, S. (2011). Stuxnet worm impact on industrial cyber-physical system security.

[3] SAnatoly Kurmanaev and Isayen Herrera. (2019). No End in Sight to Venezuela's Blackout, Experts Warn. nytimes.com.

[4] Marton, I., Sanchez, A. I., Carlos, S., & Martorell, S. (2013). Application of Data Driven Methods for Condition Monitoring Maintenance. 4th IEEE Conference on Prognostics and System Health Management (PHM). IEEE.

[5] Caselli, M., Zambon, E., & Kargl, F. (2015). Sequence-aware intrusion detection in industrial control systems. 13-24.

[6] Vollmer, T., Alvesfoss, J., & Manic, M. (2011). Autonomous rule creation for intrusion detection.

[7] Morris, T., & Gao, W. (2014). Industrial control system traffic data sets for intrusion detection research. International Conference on Critical Infrastructure Protection, 8, 65-78.

[8] Bay, S. D., Kibler, D., Pazzani, M. J., & Smyth, P. (2000). The uci kdd archive of large data sets for data mining research and experimentation. ACM SIGKDD Explorations Newsletter.

[9] Gao, W. . (2013). Cyberthreats, attacks and intrusion detection in supervisory control and data acquisition networks. Dissertations & Theses - Gradworks.

[10] Chen X Y. (2014). Research on Network Attack Model Based on Temporal Logic. (Doctoral dissertation, Zhengzhou University).

[11] Schneier B. (1999). Attack trees:modeling security threats. Dr Dobbs Journal, 24(12), 4-6.

[12] Hochreiter, S. , & Schmidhuber, J. . (1997). Long short-term memory. Neural Computation, 9(8), 1735-1780.

[13] Goh, J. , Adepu, S. , Junejo, K. N. , & Mathur, A. . (2016). A Dataset to Support Research in the Design of Secure Water Treatment Systems. The 11th International Conference on Critical Information Infrastructures Security. Springer, Cham.

CYBER SECURITY SITUATIONAL AWARENESS JOINTLY UTILIZING BALL K-MEANS AND RBF NEURAL NETWORKS

CHENG PENG[1], WANG YONGLI[1,*], YAO BOYI[1], HUANG YUANYUAN[1], LU JIAZHONG[1], PENG QIAO[1]

[1]School of Cybersecurity, Chengdu University of Information Technology, Chengdu 610225, China
E-MAIL: 156935815@qq.com

Abstract:

Low accuracy and slow speed of predictions for cyber security situational awareness. This paper proposes a network security situational awareness model based on accelerated accurate k-means radial basis function (RBF) neural network, the model uses the ball k-means clustering algorithm to cluster the input samples, to get the nodes of the hidden layer of the RBF neural network, speeding up the selection of the initial center point of the RBF neural network, and optimize the parameters of the RBF neural network structure. Finally, use the training data set to train the neural network, using the test data set to test the accuracy of this neural network structure, the results show that this method has a greater improvement in training speed and accuracy than other neural networks.

Keywords:

Situation awareness; RBF neural network; Ball k-means clustering;

1. Introduction

As network security plays an important role in national defense, enterprises, and government departments, situational awareness has emerged in the field of network security. Cyberspace is becoming more and more complex, attack technologies are emerging one after another, and automated attack tools continue to emerge, traditional network defense technologies have become inadequate. It is difficult to solve complex problems from a few network defense technologies alone. Situational awareness extracts, learns, and predicts network security trends for the elements that affect network security, so as to detect network attacks and attack events in a timely manner. deal with it.

In 1995, Endsley first proposed a human decision model in the paper, namely Endsley three-level model, the content includes situational element awareness (information collection), situation understanding (information processing), situation prediction (information output). in 1999, Tim Bass proposed the concept of cyber situational awareness, combining cyber security with situational awareness for the first time, and proposed that the fusion of multiple sensor data is the difficulty of cyber security situational awareness. With this issue raised, cyber security researchers at home and abroad started with the research of network security situational awareness system.

2. Research status

Gan [1] et al proposed a network security situation prediction model based on RAN-RBF neural network. This model uses a resource allocation algorithm to cluster data, find out the initial center of the RBF neural network, and then use the improved the particle swarm algorithm optimizes some parameters of the neural network, which is more accurate than the prediction result of the k-means RBF neural network.

Gao [2] et al used a hybrid hierarchical genetic algorithm to optimize the parameters of the RBF neural network, and coded the center of the hidden layer of the RBF network and the width parameters as independent units separately, although such experimental results will improve the accuracy of training prediction. But it increases the time complexity of the algorithm.

Zhang[3] et al proposed a game model, which based on the spread of threats, to threaten, ordinary users and administrators Markov game analysis model is established as the core ,determine network security behaviors and give an assessment of system vulnerability, the short coming of the proposed reinforcement plan is that the evaluation efficiency in the real environment is low, and it is difficult to make detailed judgments on network security behaviors, which needs to be improved.

Joel Brynielsson [4] et al discretized the network security indicator data, used different evaluation methods to classify the network security situation indicators, and obtained the final situation awareness indicators through the combination of game theory and Bayesian networks. Evaluation of this model the results are relatively objective and accurate, and the network security situation can be grasped in real time, but in the real network environment, the

assessment results are still biased.

Regarding the current deficiencies in the research of network security situation awareness, this paper proposes a network security situation model based on fast clustering RBF neural network, using the ball k-means fast clustering algorithm to cluster the original data, and find the RBF neural the initial center of the network, and then optimize the structural parameters of this RBF neural network.

3. RBF neural networks

3.1. RBF neural network structure

RBF is a special forward feedback neural network that can approximate arbitrary nonlinear functions. This structure has only 3 layers, including the input layer, the hidden layer, and the output layer. The input layer is composed of n perceptual units, which are responsible for inputting data to the neural network. The hidden layer uses radial basis functions to directly map the input vector to the high-dimensional space without being connected by weights. The hidden layer to the output layer changes linearly. The change of the weight depends on the least square method to get the loss function, so as to get the change rule of the weight and the bias, so as to update the weight and the bias continuously until these values are not changing or the error is within a threshold Inside. The final trained RBF neural network model is obtained.

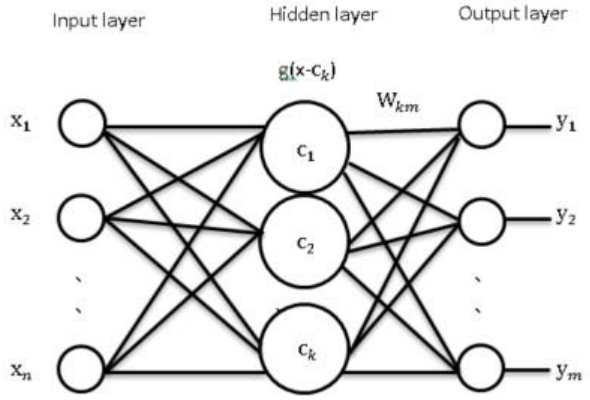


Fig.1 Structure diagram of RBF neural network

The number of input layer nodes of the RBF neural network n depends on the dimensionality of the data, c_i in the implicit layer is the center of the radial basis function g, The radial basis function consists of three types: Pseudo-quadratic functions, Gaussian Functions, Inverting the S-Function, the most mainstream is the Gaussian function $g(x,ci) = \exp(-\frac{||x-ci||}{2*\sigma*\sigma})$, i=1,2…k. Determining the center of the radial basis function is difficult, the choice of the initial center point directly affects the execution time of the neural network. A weight of matrix of weights k*m from the implied layer to the output layer, the output is $y_m = \sum_{i=1}^{k} w_{im}\, g_i, w_{im}$ is the connection weight of the i-th neuron of the implicit layer to the m-th neuron of the implicit layer.

The selection of the initial center point of the RBF neural network directly affects the operation efficiency of the algorithm. A good method to quickly select the most appropriate implicit layer node is presented in literature [5]. The original k-means algorithm randomly selects K (the number of classes into which K is divided) points as cluster centers, calculate the distance from each remaining point to each cluster center, take the minimum distance, and place it into a class, thus dividing it into K classes. But that doesn't make it right, recalculate the center of mass for each cluster (the center of mass is calculated as x as the average of the x coordinates of the points of the cluster and y as the average of the y coordinates of the points of the cluster), calculate the distance from each remaining point to each center of mass and take the minimum distance until the result is the same as the previous clustering.

3.2. Ball Cluster Division

The concepts of cluster, neighborhood cluster search, and cluster partitioning were introduced in literature[5] to improve the original k-means algorithm, in order to dispense with distance calculations for points that are very far from the center, a cluster Ca and a neighboring cluster Cb are defined here, if half of the distance between the centers of the two clusters is less than the radius of the two clusters, then the two clusters are said to be adjacent to each other. If half of the distance between the centers of the two clusters is less than the radius of cluster Ca and greater than the radius of cluster Cb, then it can be assumed that Cb is a neighboring cluster of Ca and Ca is not a neighboring cluster of Cb. If half of the distance between the centers of the two clusters is greater than the radius of the two clusters, then the two clusters are not considered to be in proximity. The expression formula is: $\frac{1}{2}$||Ca-Cb||<ri, because the points are not moving, they can only be partitioned into clusters using the above definition.

3.3. Division of area

Regions are divided here into stable and active domains, definition of stable domains: Ca is the ball cluster to be queried, {SetCa} represents the set of Ca adjacent cluster centers, if this set is not an empty set, then it can be determined that the stable region of Ca is a spherical region

with a radius of $\frac{1}{2}$min(||ca- cb||) cbNCi. Other regions that are not in the stable domain are defined as active domains. So the points in the stable domain are not computed in the next iteration.

3.4. Division of ring domain

Neighboring domains are generated from the set of neighboring clusters in the active domain, and the number of nearest neighbors within each ring is further reduced, thus further reducing the number of distance calculations. Finding each neighboring cluster requires calculating the distance between the centers of two clusters, the time complexity is O(k^2), after the division of the domain, the non-neighbor relationship in the next iteration can be calculated in advance, and the calculation of the distance between the centers of the two clusters can be avoided.

A stable cluster of balls will not be calculated in the next iteration, stable clusters are not computed in the next iteration. A stable cluster is one in which no dots move in and no dots move out in this iteration. With each iteration, the number of stable clusters increases until the entire largest cluster is stable. With each iteration, the time complexity of the ball k-means algorithm becomes sub-linear and the ball k-means algorithm executes faster and faster.

4. Experimental Analysis

4.1. Data Set

The training set data in this paper is from CICIDS2017. This dataset is large in capacity, has many traffic categories, covers a variety of known attacks, it can fully reflect current network security trends, and has multiple feature sets and metadata to fully emulate real-world network traffic. In order to avoid the difficulty of handling multivariate data and to speed up the process of finding the optimal solution, all data are normalized here. For normalization of the raw data, the formula is: $xi = \frac{\text{x-xmin}}{\text{xmax-xmin}}$

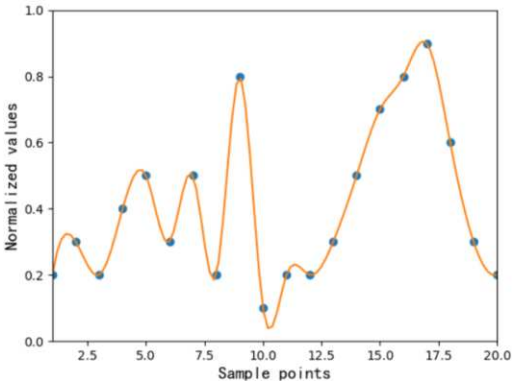


Fig.2 Normalized value

4.2. Simulation and contrast experiment

In Simulation Experiments, the first step is to determine the appropriate data center for the radial basis function of the nodes of the implied layer using the ball k-means clustering algorithm, and to determine the expansion constant of the implied layer based on the distance between the centers, the formula is $\theta = \frac{\text{dmax}}{\sqrt{2M}}$, d_{max} is the maximum distance between the selected data centers; M is the number of data centers. The second step is to train the output weights using the gradient descent method with the RBF neural network, and the resulting nonlinear function continuously fits the data set. When the overall error reaches the minimum value, the function converges, and the training is completed. Use a portion of the CICIDS2017 dataset as a training set to train this improved neural network model, adjust the neural network model's parameter configuration during the training process to obtain the best model, and then use the rest of the data set as a test set to test the accuracy of this improved neural network model. Take the value after 5 consecutive processes to predict the next potential value, the input layer node is 5, the output value is divided into 10 categories, the result is a decimal number from 0 to 1 as the potential value, so the number of implicit layer nodes is 10, the output node is 1, so the structure of the whole neural network is 5-10-1.

In order to highlight the superiority of this improved neural network, the same comparison between RBF neural network and BP neural network is performed here and the predicted results are as follows:

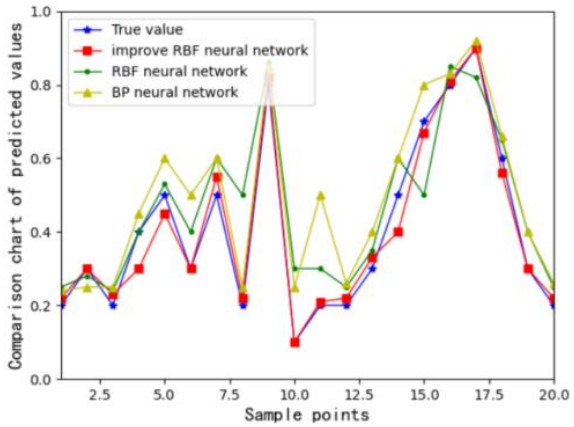


Fig.3 Forecast results

In order to demonstrate the superiority of the improved RBF neural network, the Average Relative Error (ARE) metric was selected for quantitative analysis, and the comparison results show that the ball k-means optimized RBF neural network significantly improves the prediction accuracy.

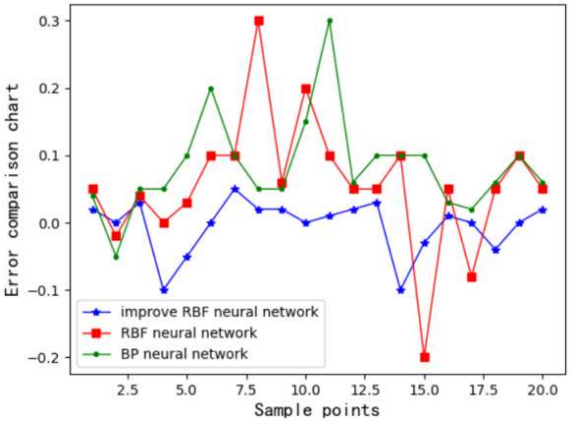


Fig.4 Error comparison

To demonstrate the response speed of the improved RBF neural network, the speed comparison with the RBF neural network and BP neural network is made here, and it is obvious that the improved RBF neural network operates faster than the other two neural networks.

Table 1 Speed Comparison

Demision	RBF neural network	BP neural network	Improve RBF neural network
200	253ms	375ms	136ms
500	336ms	586ms	203ms
1000	482ms	734ms	322ms

5. Conclusions

This paper presents a ball k-means algorithm optimized cyber security situational awareness approach for RBF neural networks, by combining the ball k-means algorithm with the RBF neural network, the ball-cluster search, ball-cluster partitioning concept is used to perform a fast search for the initial center of the RBF neural network, the fast convergence of RBF neural networks is more suitable for real-time network security situational awareness applications than the slow speed of the multilayer implicit layer of BP neural networks. Through the comparison of experimental data, the network security situational awareness model in this paper is more accurate, faster, and has a lower average relative error, which helps network administrators understand network security risks in a timely manner and make better network security decisions more quickly.

Acknowledgements

We would like to express my deepest gratitude for the help of my teachers and classmates, without whom I could not have completed my thesis. The authors really appreciate the handling associate editor and all innominate reviews for their valuable comments. This work is supported by the National Natural Science Foundation of China (No.62076042, No.61572086), the Key Research and Development Project of Sichuan Province (No. 2020YFG0307, No. 2018TJPT0012), the Key Research and Development Project of Chengdu (No. 2019-YF05-02028-GX), the Innovation Team of Quantum Security Communication of Sichuan Province (No.17TD0009), Sichuan Science and Technology Program under Grants 2018RZ0072, 20ZDYF0660, the Foundation of Chengdu University of Information Technology under Grant J201707, the National Key R&D Program of China under Grant (No.2017YFB0802300), in part by Foundation of Chengdu University of Information Technology under Grant J201707, in part by College Students & apos; innovation project of Chengdu University of Information Technology under Grants 202010621260 and 202010621268.

References

[1] Wen-Dao G , Cheng Z , Bo S,Network Security Situation Prediction Model Based on RAN-RBF Neural Network, Computer ence, 2016.

[2] GAO Yanhe.The RBF neural network optimization and application based on hybrid hierarchy genetic algorithm, Chengdu,2004.

[3] Yong Z ,Xiaobin T,Xiaolin C, et al. Network Security Situation Awareness Approach Based on Markov Game Model ,Software Journal,pp. 495 -508,2011.
[4] JoelB,Stetan A Bayesian games for threat prediction and situation analysis, December 2009.
[5] S. Xia *et al*., "A Fast Adaptive k-means with No Bounds," in IEEE Transactions on Pattern Analysis and Machine Intelligence, Chongqing,2020.
[6] Lixia X , Yachao W , Jinbo Y U, Network security situation awareness based on neural networks, Journal of Tsinghua University, Beijing, pp.1750-1760,2013.
[7] Xia S , Liu Y , Ding X , Wang G et al, Granular Ball Computing Classifiers for Efficient, Scalable and Robust Learning, Information Sciences, pp. 136-152,2019.
[8] Xiaowu Liu, Jiguo Yu, Weifeng Lv, et al. Network security situation: From awareness to awareness control,Journal of Network and Computer Applications,pp. 139, 15-30,2019.
[9] Lei, H, Li, HL, Wei, ZH, et al. Summary of research on IT network and industrial control network security assessment. In: 2019 IEEE 3rd information technology, networking, electronic and automation control conference (ITNEC), Chengdu, pp.1203–1210, March 2019.
[10] Tianfield H,Cyber security situational awareness,In: 2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData), Chengdu, pp.782–787. December 2016.
[11] Jin YH, Shen YJ, Zhang GD, et al,The model of network security situation assessment based on forest. In: 2016 7th IEEE international conference on software engineering and service science (ICSESS), Beijing, pp.977–980, August 2016.
[12] Shi LL and Chen J. Assessment model of command information system security situation based on twin support vector machines. In: 2017 international conference on network and information systems for computers (ICNISC), Shanghai, pp.135–139, April 2017.

A SECURE AUTHENTICATION SCHEME FOR MOBILE CLOUD COMPUTING AGAINST CCA

MD JAKIR HOSSAIN[1], CHUNXIANG XU[1], CHUANG LI [1]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China
E-MAIL: jakir.cse.metrouni@gmail.com, chxxu@uestc.edu.cn, leeChuanglc@163.com

Abstract:

Authentication schemes employing identity-based encryption are widely used in mobile cloud computing environments. It enables users to get umpteen services from different cloud servers by registering only once with a third-party. However, in existing schemes, the security against chosen-ciphertext attacks and malicious private key generator is not well-considered. These security pitfalls may cause security and privacy issues in some application scenarios since an active attacker can send a number of adaptively chosen ciphertext and tries to distinguish the target ciphertext; succeeds may cause the exposure of the underlying secret key. In this paper, we propose a secure and efficient authentication scheme for mobile cloud computing with security against chosen-ciphertext attacks and malicious private key generator based on adaptive one-wayness trapdoor function and learning-parity with noise hardness assumption. Our comprehensive security proof demonstrates that our scheme is indistinguishable against chosen-ciphertext attacks.

Keywords:

Learning-parity with noise; Chosen ciphertext attacks; Identity-based encryption; Private key generator

1. Introduction

With the rapid development of mobile applications and cloud computing emerges a revolutionary technology called mobile cloud computing. This framework facilitates mobile users to outsourced their data to the cloud server and can be accessed when necessary. Secure authentication schemes are obvious to ensure secure communication between mobile users and cloud servers. However, existing schemes either fail to achieve chosen-ciphertext attacks (CCA) security or require quite a large number of pairing operations.

To mitigate these issues, a comprehensive range of research works [1] have been introduced to design an IND-CCA secure public-key encryption (PKE) scheme by employing a simple and derandomization technique. However, in the standard model, it is impossible to construct an IND-CCA secure PKE scheme using a simple derandomization technique [2]. The IND-CCA security problem is partially solved by [3]. In addition, to ensure security against malicious authority, researchers employed an identity certifying authority (ICA) with a private key generator (PKG) to protect the user's privacy against malicious PKG. Despite the desired advantage from the existing schemes, they need strong additional requirements of randomness reusability; the instantiations of these approaches are limited to specific number-theoretic assumptions. In addition, existing schemes require quite a large number of pairing operations during decryption [4].

This paper presents an efficient and secure authentication scheme for mobile cloud computing with security against CCA based on learning-parity with noise (LPN) hardness assumption [5]. Our scheme achieves pseudorandom ciphertext property and randomness-recoverability. Specifically, the contribution of this paper is two-folded:

We propose a secure authentication scheme for the mobile cloud computing environment. The proposed scheme is constructed based on adaptive one-wayness trapdoor function and learning-parity with noise hardness assumption; therefore, our scheme achieves security against CCA.

We define the formal security model of CCA of our scheme and present security proof under that model.

2. Problem statement

System Model: As shown in Figure 1, there are four entities in our proposed scheme: User, cloud server, ICA, and PKG.
User: The set of users who want to take services from cloud servers must register with the trusted authority (TA). The user can be accessed all cloud servers associated with TA.
Cloud server: The cloud server is the cloud service provider, which has storage servers and massive computing power. The cloud server registered with TA before providing services.

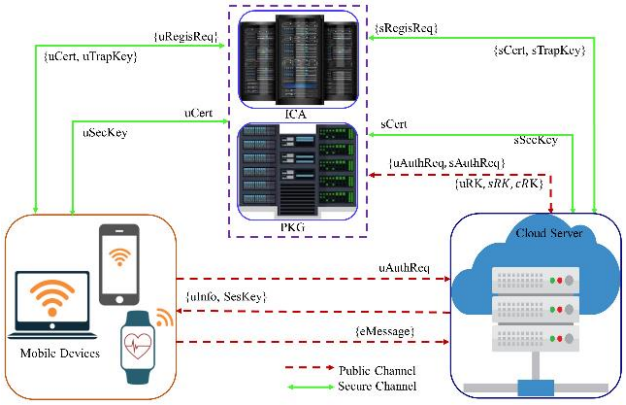


Fig.1 System model

Trusted authority (TA): To enhance trust, TA employs ICA with PKG. ICA generates a certificate and a trapdoor key for the given identity, and PKG generates the master secret key and certificate-specific key for the given certificate. PKG verifies both the user and cloud server during the authentication phase. Finally, PKG generates two random numbers that are used to generate the session key.

2.1. Threat model

In the adversary model, we consider a probabilistic polynomial time-bounded adversary who has the ability to encrypt the message of its choice and can decrypt the ciphertext of its choice. An active attacker can send a number of adaptively chosen ciphertext and tries to distinguish the target ciphertext.

2.2. Design goals

A secure authentication scheme should achieve the following goals.

Security: The authentication scheme for mobile cloud computing should ensure the security against CCA, i.e., an active attacker can send a number of adaptively chosen ciphertext of its choice to the challenger, but it will reveal nothing about the underlying secret key.

Efficiency: The authentication scheme should provide better efficiency.

3. Proposed scheme

A. **Notations and conventions**: We use $\mathbb{N}$ to represent natural numbers, for $n \in \mathbb{N}$, we define $n := \{1, 2, \ldots n\}$. We use S to represent a discrete finite set, where $|S|$ represents its size. We use $x \xleftarrow{r} S$ to present x is chosen uniformly at random from S. $x||y$ represents the concatenation of string x and y. $y \leftarrow A(x)$ denotes on input x and A, a function or a probabilistic algorithm A outputs y. $y \leftarrow A(x; r)$ denotes randomness r is used to output y. λ denotes the security parameter. $f(\lambda) = \mathbf{negl}(\lambda)$ denotes $f(\lambda)$ is the negligible function. $\mathbf{poly}(\cdot)$ denotes unspecified positive polynomial.

Alg.1 Encryption Algorithm

Input: params, X_m, x
Output: Ciphertext y

Run sampling algorithm to generate x
Compute $CT_{SKE} \leftarrow E((r_i^{s_i})_{i\in[n]}||X_m||k; r_{SKE})$
for $i \leftarrow 1$ *to* n **do**
  $(ct_i^{s_i} k_i^{s_i}) \leftarrow Encap(PK_i^{s_i}, r_i^{s_i})$
  $ct_i \leftarrow ct_i^{s_i} + s_i \cdot C_i$
  Set: ct_i^0 if $s_i = 0$
  Set: $ct_i^1 + C_i$ if $s_i = 1$
Compute h$\leftarrow H(hk, (ct_i)_{i\epsilon[n]}||ct_{SKE})$
for $i \leftarrow 1$ *to* n **do**
  Compute: $T_i \leftarrow (K_i^{s_i} + s_i \cdot (A_i + B \cdot h))$
  Set: k_i^0 if $s_i = 0$
  Set: $k_i^1 + A_i + B.h$ if $s_i = 1$
Return y $\leftarrow ((ct_i, T_i)_{i\in[n]}, ct_{SKE})$

B. **Setup** $(\mathbf{1}^{\lambda})$: Chooses $2n$ public keys $(pk_i^v)_{i\in[n],\ v=\in\{0,1\}}$ and corresponding secret key $(sk_i^v)_{i\in[n],\ v=\in\{0,1\}}$, secret keys $s = (s_1, \ldots, s_n) \in \{0,1\}^n$, where $[n] := \{1, \ldots, n\}$, the output of the encryption algorithm is $2n$ ciphertext represented as (ct_i^0, ct_i^1), an encoding (ct_i^0, ct_i^1) signals α when ct_i^{α} encrypts 1. A tag $(T_i)_{i\in[n]}$ is added with each encoding. Let the identity $I\mathcal{D} = \{0,1\}^*$ is chosen from the identity space $I\mathcal{D}$.

3.1. Registration phase

A. **User registration:**

Step1. U_i chooses ID_i from $I\mathcal{D}$ and sends a registration request to ICA.

Step2. Upon receiving ID_i, ICA informs U_i's ID_i is duplicate if ID_i already exists and terminates the registration process. Otherwise, ICA generates Cert_i and a trapdoor key T_{P_i}. ICA then sends $\{\mathrm{Cert}_i, T_{P_i}\}$ to U_i.

Step3. Upon receiving $\{\mathrm{Cert}_i, T_{P_i}\}$, U_i sets $M_{U_i} = \mathrm{Cert}_i$ and sends M_{U_i} to PKG.

Step4. On receiving M_{U_i}, PKG rejects the registration process if Cert_i exists. Otherwise, PKG generates M_{PKG_i}, computes $\beta_i = \mathrm{M}_{PKG_i} \oplus h(T_{reg}||\rho)$, and sends $\{\mathrm{M}_{PKG_i}, \beta_i\}$ to U_i and stores $\{\mathrm{Cert}_i, \beta_i\}$ on its database.

Step5. Upon receiving M_{PKG_i}, U_i 's device computes

$e_{ID_i} = T_{P_i} \oplus \mathrm{M}_{PKG_i}$. U_i inputs the chosen password PW_i and U_i's device computes $d_i = h(PW_i||b_i)$, where b_i is a random number, $BFU_i = h(ID_i \oplus d_i) \bmod f_i$, where f_i is the medium integer $2^4 \le f_i \le 2^8$. U_i's device finally computes $U_{C_i} = BFU_i \oplus \mathrm{Cert}_i$, $U_{T_i} = BFU_i \oplus \mathrm{T}_{P_i}$, $U_{M_i} = BFU_i \oplus M_{PKG_i}$, and $U_{K_i} = BFU_i \oplus \mathrm{e}_{ID_i}$.

Step6. U_i 's device generates a secret key $U_{sec_i} \leftarrow KKG(1^\lambda)$ and publishes the corresponding public key U_{pub_i} to all entities in the system. Finally, U_i's device securely maintains $\{U_{c_i}, U_{T_i}, U_{K_i}, U_{sec_i}, b_i, f_i, \beta_i\}$.

Alg.2 Decryption Algorithm

Input: params, y
Output: Ciphertext y
$((ct_i, T_i)_{i\in[n]}, ct_{SKE}) \leftarrow$ y
Compute: $h \leftarrow H(hk, (ct_i)_{i\in[n]})||CT_{SKE}$
for $i \leftarrow 1$ *to* n **do**
  $s_i \leftarrow Decap(sk_i^0, ct_i =? T_i)$
  Set: 0 if $Decap(sk_i^0, ct_i = T_i)$
  Set: 1 *Otherwise*
Retrieve: $S = (S_1, S_2, \dots, S_n) \in \{0,1\}^n$
Recover randomness: $(m, r_{SKE}) \leftarrow RD(s, ct_{SKE})$
Parse: m as $(r_i^{s_i})_{i\in[n]} \in \{0,1\}^{n\cdot\lambda}$
$k \in \{0,1\}^\ell$ and X_{m_i}
Compute: X$\leftarrow (S, (r_i^{s_i})_{i\in[n]}, k, r_{SKE})$
if Eval(params, x) = y **then**
  Return x, X_m
Else
  Otherwise, return: $\perp$

B. **Cloud server registration:**

Step1. Server CS_j chooses her/his ID_j and ID_j to ICA.

Step2. Upon receiving ID_j, ICA informs that the server identity is duplicate if ID_j already exists. Otherwise, ICA generates $\{\mathrm{Cert}_j, T_{P_j}\}$ and sends $\{\mathrm{Cert}_j, T_{P_j}\}$ to CS_j.

Step3. Upon receiving $\{\mathrm{Cert}_j, T_{P_j}\}$, CS_j sets the message $M_{S_j} = \mathrm{Cert}_j$ and sends M_{S_j} to PKG.

Step4. On receiving M_{S_j}, PKG rejects the registration process if Cert_j exist. Otherwise, PKG runs *Algorithm 1* and returns M_{PKG_j}, β_j to CS_j. PKG then stores Cert_j, β_j.

Step5. Upon receiving M_{PKG_j}, CS_j computes $e_{ID_j} = T_{P_j} \oplus M_{PKG_j}$, generates $S_{sec_j} \leftarrow KKG(1^\lambda)$, and publishes the corresponding public key S_{pub_j} to all entities in the system. Finally, S_j securely maintains $\{e_{ID_j}, \mathrm{Cert}_j, S_{sec_j}, \beta_j, M_{PKG_j}\}$.

3.2. Authentication phase

The authentication phase of our scheme is described below.

Login:

Step1. U_i inputs ID_i and PW_i through an application *App* installed on her/his device.

Step2. On receiving ID_i and PW_i, *App* computes $d_i = h(PW_i||b_i)$, $BFU_i = h(ID_i \oplus d_i) \bmod f_i$ and retrieves, $\mathrm{Cert}_i' = BFU_i \oplus U_{C_i}$, $T_{P_i} = BFU_i \oplus U_{T_i}$, $e_{ID_i} = BFU_i \oplus U_{K_i}$, $M_{PKG_i} = BFU_i \oplus U_{M_i}$, and $\delta_i = \beta_i \oplus M_{PKG_i}$. If BFU_i is valid, U_i can login to the system and retrieve $\mathrm{Cert}_i, T_{P_i}\delta_i$. Otherwise, *App* rejects the login request.

Verification:

Step1. To get service from CS_j, U_i runs *Algorithm 1* and encrypt $X_{m_i} = \mathrm{Cert}_i, \delta_i$. On input system parameters *param*, x, and X_{m_i}, *Algorithm 1* outputs $\mathrm{y}_i \leftarrow ((ct_i, T_i)_{i\in[n]}, ct_{SKE_i})$. U_i then sends y_i to CS_j.

Step2. On receiving y_i, CS_j computes $\delta_j = \beta_j \oplus M_{PKG_j}$. CS_j runs *Algorithm 1*, which takes *params*, X_{m_i}, and x as input, and outputs $\mathrm{y}_j \leftarrow ((ct_j, T_j)_{j\in[n]}, ct_{SKE_j})$. Finally, CS_j sends $\{\mathrm{y}_i, \mathrm{y}_j\}$ to PKG.

Step3. On receiving $\{\mathrm{y}_i, \mathrm{y}_j\}$, PKG can retrieves X_j by running *Algorithm 2* if all parameters are valid. PKG then parses X_{M_j} as $\{\mathrm{Cert}_j', \delta_j'\}$.

Step4. On input $\{\mathrm{Cert}_j', \delta_j'$, PKG first checks whether Cert_j' exists on its local database. If it does not exist, PKG terminates the authentication process. Otherwise, PKG computes $\delta_j = \beta_j \oplus M_{PKG_j}$ and checks whether $\delta_j' = \delta_j$ holds. If it holds, PKG picks uniformly random $z_j \leftarrow \{0,1\}^\lambda$.

Step5. Afterward, PKG decrypts the user's ciphertext and parses $\{\mathrm{Cert}_i', \delta_i'\}$ from X_{m_i}.

Step6. On inputs$\{\mathrm{Cert}_i', \delta_i'\}$, PKG verifies the user using the aforementioned procedures and computes $\delta_i = \beta_i \oplus M_{PKG_i}$. Afterward, PKG picks uniformly random $z_i \leftarrow \{0,1\}^\lambda$ if $\delta_i' = \delta_i$ holds.

Step7. Finally, PKG computes $C_{PKG_i} = z_i \oplus h(X_{m_i}')$, $C_{PKG_j} = z_j \oplus h(X_{m_j}')$, $Com_{PKG} = h(z_i) \oplus h(z_j)$, and sends $\{C_{PKG_i}, C_{PKG_j}, Com_{PKG}\}$.

Mutual Authentication:

Step1. On receiving $\{C_{PKG_i}, C_{PKG_j}, Com_{PKG}\}$, CS_j retrieves secret as $z_j = C_{PKG_j} \oplus h(X_{m_j})$ and computes $NS_{ID_j} = h(e_{ID_j}||\mathrm{a}_j)$ where a_j is a random number. CS_j then runs *Algorithm 1* to generate $\mathrm{y}_{su} \leftarrow ((ct_j, T_j)_{j\in[n]}, ct_{SKE_j})$. Finally, CS_j sends y_{su} to U_i, which contains $X_{m_{su}} =$

$\{NS_{ID_j}, C_{PKG_i}, Com_{PKG_i}\}$.

Step2. On receiving y_{su}, U_i decrypt the ciphertext and parses $\{NS'_{ID_j}, C'_{PKG_i}, Com'_{PKG_i}\}$ from $X_{m_{su}}$. U_i retrieves $z_i = C_{PKG_i} \oplus h(X_{m_i})$, computes $h(z_j) = h(z_i) \oplus Com_{PKG}$ and checks whether $h(z'_j) = h(z_j)$ hold. If it holds, U_i computes $NS_{ID_i} = h(e_{ID_i}||a_i)$ and $SK_{ij} = h(z_i||z'_j||NS_{ID_i}||NS_{ID_j})$. U_i then runs *Algorithm 1* to encrypt $X_{m_{us}} = \{NS_{ID_i}, z_i, SK_{ij}\}$. The output of *Algorithm 1* is y_{us}, which is sent to CS_j.

Step3. On receiving y_{us}, CS_j runs *Algorithm 2* and parses $\{NS'_{ID_i}, z'_i, SK'_{ij}\}$. CS_j computes $h(z_i) = h(z_j) \oplus Com_{PKG}$ and checks whether $h(z'_i) = h(z_i)$ hold. If it holds, CS_j computes $SK_{ij} = h(z'_i||z_j||NS_{ID_i}||NS_{ID_j})$ and checks whether $SK_{ij} = SK'_{ij}$ hold. If the condition holds, CS_j agrees with the generated session key.

4. Security analysis

The security analysis of our scheme is as follows.

Theorem 1. *An authentication scheme (AKE) is called INDCCA secure if and only if the key encapsulation mechanism (KEM) is almost-all-keys correct and IND-CPA secure, secret key encryption is one-time projection-key dependent message (P-KDM) secure, and hash is the target collision resistance.*

Proof: Consider key encryption mechanism $\epsilon: \mathbb{N} \to [0,1]$, where ϵ -almost-all-keys correct. A PPT adversary can make $q_{dec} = q_{dec}(\lambda) > 0$. There exist PPT adversaries $\beta_{tcr}, \{\beta^j_{cpa}\}_{j\epsilon[4]}, \beta'_{cpa}$ and single KDM query β_{KDM} which satisfies the following equation.

$$\begin{aligned}\frac{1}{2}Adv^{cca}_{AKE_{cca,\mathcal{A}}}(\lambda) \leq\ & Adv^{tcr}_{hash,\beta_{tcr}}(\lambda) \\ &+ \sum_{j\epsilon[4]} Adv^{mcpa}_{KEM,n,\beta^j_{cpa}}(\lambda) \\ &- q_{dec}.Adv^{mcpa}_{KEM,n,\beta'_{cpa}}(\lambda) \\ &+ Adv^{mcpa}_{SKE,\mathcal{P},\beta_{KDM}}(\lambda) + 8\epsilon + n.2^{-\lambda+3} \\ &+ n(q_{dec}+1).2^{-4\lambda+1}.\end{aligned}$$

We consider the following games to prove the theorem.

Game0: In order to make the identical distribution of (PK, SK, CT^*, k^*_b), we change the ordering of operations for how to challenge ciphertext/ session key pair (CT^*, k^*_b) and a key pair (PK, SK) is generated. This game signifies the original scheme with random oracles.

$$Adv^{cca}_{AKE_{cca,\mathcal{A}}}(\lambda) = 2 \times P_r[S_0] - 1 \quad (1)$$

Game1: The variation of Game0 and Game1 is, $\mathcal{A}'s$ decapsulation query (CT=(ct^0_i, ct^1_i, T_i), ct_{SKE}) satisfies h = H(CT=(ct^0_i, ct^1_i, T_i), ct_{SKE})= h^*, thereby decapsulation query returns $\perp$ to $\mathcal{A}$.

$$\begin{aligned}|P_r[S_0] - P_r[S_1]| \leq\ & Adv^{tcr}_{hash,\beta_{tcr}}(\lambda) \\ &+ \sum_{j\in[n]} Adv^{mcpa}_{KEM,n,\beta^j_{cpa}}(\lambda) \\ &- q_{dec}.Adv^{mcpa}_{KEM,n,\beta'_{cpa}}(\lambda) + 3\epsilon + n \\ &\cdot 2^{-\lambda+1} + n(q_{dec}+1)\cdot 2^{-4\lambda}\end{aligned} \quad (2)$$

Game2: The only exception of Game1 and Game2 is how A_i's for every position the secret $i \epsilon S_{zero}$ is generated where $A_i \leftarrow k^0_i - k^1_i - B \cdot h^*$. Therefore, the probability of winning this game is,

$$|P_r[S_1] - P_r[S_2]| \leq Adv^{mcpa}_{KEM,n,\beta'_{cpa}}(\lambda) \quad (3)$$

Game3: In this game, the oracle returns $\perp$ if $h = h^*$ on answering decapsulation query; otherwise, the oracle uses an alternative algorithm and key SK' to output k. The decapsulation oracle answer queries without using sk^0 due to this modification. Therefore, the winning probability is,

$$|P_r[S_2] - P_r[S_3]| \leq 2\epsilon + n \cdot 2^{-\lambda+1} \quad (4)$$

Game4: The variation of Game3 and Game 4 is how A_i's for every position the secret $i \in S_{one}$ is generated. All $(A_i)_{i\in[n]}$ are generated. In addition, $T^*_i = k^{*0}_i$ holds for all $i \in [n]$ no matter whether $s^*_i = 0$ or $s^*_i = 1$. Therefore, the probability of winning this game is,

$$|P_r[S_3] - P_r[S_5]| = Adv^{mcpa}_{KEM,n,\beta'_{cpa}}(\lambda) \quad (5)$$

Game5: The only exception of Game4 and Game5 is, how the challenge bit b is erased from the ciphertext ct^*_{SKE} in Game5. In this game the challenge ciphertext CT^* is generated from $ct^*_{SKE} \leftarrow E(s^*, 0^{n\cdot\lambda+\ell})$ instead of $ct^*_{SKE} \leftarrow E(s^*, (r_i{}^{*(s^*_i)})_{i\in[n]}||k^*_1)$. Therefore, the winning probability of winning the game by a PPT adversary is,

$$|P_r[S_4] - P_r[S_5]| = Adv^{mcpa}_{KEM,n,\beta'_{cpa}}(\lambda) \quad (6)$$

Finally, rearranging the terms, we obtain the desired result, which proves theorem 1. Therefore, $\mathcal{A}$'s has no advantage in winning and Game5. Hence, $P_r[S_5] = \frac{1}{2}$.

5. Conclusion

In this paper, we have proposed an authentication scheme for mobile cloud computing based on learning-parity with noise hardness assumption, which achieves security against CCA. The proposed scheme enables honest mobile users to be accessed their cloud data securely. We provide detailed security proof of the proposed scheme, which demonstrates that our scheme achieves security against CCA.

For future work, we will analyze the security against the

malicious user, ICA, and PKG. Specifically, PKG potentially has the power to decrypt all the ciphertext since PKG can generate the private key pair for the given identity. Therefore, users and cloud servers are always worried about communication privacy against malicious PKG. It is an open challenge to secure authentication scheme against PKG.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grant 61872060, the National Key RI&D Program of China under Grant 2017YFB802000, and the National Natural Science Foundation of China under Grant 61370203.

References

[1] E. Fujisaki, T. Okamoto, How to Enhance the Security of Public-Key Encryption at Minimum Cost, PKC1999, pp. 53–68, 1999.
[2] Y. Gertner, T. Malkin, S.A. Myers, Towards a Separation of Semantic and CCA Security for Public Key Encryption, TCC2007, pp. 434–455, 2007.
[3] M. Hajiabadi, B.M. Kapron, Reproducible Circularly-Secure Bit Encryption: Applications and Realizations, CRYPTO2015, pp. 224–243, 2015.
[4] Y. Lee, D.H. Lee, J.H. Park, Tightly CCA-secure encryption scheme in a multi-user setting with corruptions, DCC2020, 2433–2452, 2020.
[5] F. Kitagawa, T. Matsuda, K. Tanaka, CCA Security and Trapdoor Functions via Key-Dependent-Message Security, CRYPTO2019, pp. 33–64, 2019.

FREQUENT ITEMSETS MINING ALGORITHM BASED ON DIFFERENTIAL PRIVACY AND FP-TREE

DING ZHE[1,2], WU CHUNWANG[1], ZHAO JUN[1], LI BINYONG[1]

[1]School of Cybersecurity, Chengdu University of Information Technology, Chengdu 610225, China
[2]School of Information and software engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China
E-MAIL: dingzhe@cuit.edu.cn

Abstract:

Mining algorithm for frequent patterns is applies in many fields. Itemsets may be contain user sensitive information. And attacker with strong knowledge can steal user privacy information by analyzing mined itemsets. So, in this paper, a novel algorithm is designed to obtain *K* itemsets whose support are more than the other itemsets and guarantee security of user privacy in itemsets. The novel algorithm firstly applies exponential mechanism to truncate original transaction dataset. And then the algorithm constructs FP-tree for truncated dataset, and utilizes Laplace mechanism to obtain noise support of itemsets. Finally, according to noise support, the algorithm can obtain *K* itemsets whose support are more than the other itemsets. In the end, two public datasets are applied to evaluate utility of the algorithm. The experimental result show that the utility of the algorithm is better than the other frequent itemsets mining based on differential privacy.

Keywords:

Frequent itemsets mining; Differential privacy; Data mining

1. Introduction

Nowadays, networks operators have gathered large volumes of user data. Those network operators can make used of data mining technologies to analysis data gathered by themselves in order to obtain user's habits. And then based on those user's habits, those network operators can have provided personal services for those users [1]. But those data contain sensitive information for users. As a consequence, under the premise of guaranteeing security of user's privacy, how to find user's habits have become hotspot in academy [2].

Frequent pattern mining is applied in many fields. And frequent itemsets mining have been applied in many fields in practices [2-4]. Attacker can steal user privacy by analyzing frequent itemsets [5]. Traditional privacy scheme is applied to protect security of sensitive information [2]. But study found that attacker with stronger background information can steal sensitive information by analyzing data processed by traditional privacy scheme [3].

Differential privacy technology has guarantee security of user privacy by injecting noise to processing of mining frequent itemsets [6]. As a consequence, attacker with stronger back knowledge cannot steal sensitive information of users by analyzing mining results. For example, apple have applied technology based on differential privacy to provide services and guarantee security of user privacy [7]. As a consequence, we make used of differential privacy technology to guarantee security of sensitive information.

Although frequent itemsets mining algorithm based on differential privacy can guarantee security of user privacy, the noise injected by differential privacy technology can cause decreases of accuracy of mining result. As a result, mining result cannot contain user habits.

In this paper, an algorithm, denoted as FIMDP, is designed to obtain *K* itemsets whose support are more than the other itemsets. And FIMDP accesses differential privacy to guarantee security of user privacy. FIMDP firstly applies traditional frequent itemsets algorithm and exponential mechanism to truncate original dataset. The truncation result can contain all information in top-*K* frequent itemsets and guarantee security of privacy. Secondly, FIMDP construct FP-Tree for truncation result. And then the novel algorithm applies Laplace mechanism of differential privacy to obtain noise support of all itemsets contained in truncation result. Finally, FIMDP can obtain top *K* most frequent itemsets by analyzing noise supports.

Paper organization is shown as follows. In section 2, related works is described. In section 3, we have introduced some foundational concept used in this paper. In section 4, we have described the detail of FIMDP. And the experiment for FIMDP is described in section 5.

978-0-7381-4259-3/20/$31.00 ©2020 IEEE

2. Related works

Nowadays, attacker can steal sensitive information by analyzing frequent itemsets. As a consequence, differential privacy is applied to mine frequent itemsets. In 2006, the concept of differential privacy was proposed by Dwork in [8]. And Bhaskar applies differential privacy technology to guarantee security of mined frequent itemsets [9]. In [10], Li introduces the concept of maximal clique to process of mining frequent itemsets. And then Laplace mechanism is applied to guarantee security of mined frequent itemsets. In [11], Zeng find that the high of transaction can influences total sensitivity of differential privacy. So, Zeng proposed an algorithm which is based on truncation technology and greedy algorithm. And the algorithm applies threshold value and dynamic weight to decrease total sensitivity.

3. Preliminaries

In this section, the foundational concept used in this paper is introduced.

Definition 1 (Neighbor datasets) [6]. Let *T* and *T*' be the two datasets. If *T* can be obtained by adding or removing a record from *T*', *T* and *T*' are two neighbor datasets.

Definition 2 (Differential Privacy) [6] Let *T* and *T*' are two neighbor datasets. *K* is a randomized mechanism. *O* is output domain of *K*. If inequation (1) is satisfied, *K* satisfies $\varepsilon-$differential privacy.

$$\mathrm{P}\left[K(T)\in O\right]\le e^{\varepsilon}\cdot\mathrm{P}\left[K(T')\in O\right] \tag{1}$$

Where ε is a real number denoted as privacy budget.

Definition 3 (Global sensitivity) [6]. Let p is query function $p: T \to R^d$. *T* and *T*' is a pair of neighbor datasets. The global sensitivity for p is obtained by equation (2) and denoted as Δp.

$$\Delta p = \max_{T,T'} \left\| p(T) - p(T') \right\|_1 \tag{2}$$

Definition 4 (Exponential Mechanism) [4] Let *T* and *o* be a dataset and an output, respectively. $r(T,o)$ is the function which describe the utility for *T* and *o*. If the possibility of *o* outputted by randomized mechanism *A* satisfies equation (3), *A* satisfying $\varepsilon-$differential privacy.

$$\Pr(o) \propto \exp\left(\frac{\varepsilon \cdot u(T,o)}{2\Delta u}\right) \tag{3}$$

where Δu refers to the sensitivity of *u*.

Definition 5 (Laplace Mechanism) [4] For dataset T, *f* is a function $f: T^n \to R$. *A* is a randomized mechanism. If equation (4) is satisfied, *A* ensures $\varepsilon-$differential privacy.

$$A(T) = f(T) + Lap\left(\frac{\Delta f}{\varepsilon}\right) \tag{4}$$

$$\Pr(x \mid \lambda) = \frac{1}{2\lambda} e^{-\frac{|x|}{\lambda}} \tag{5}$$

Probability density function of $\mathrm{Lap}(\lambda)$ is obtain by equation (4).

Theorem (Sequential Composition) [4]: For dataset *D*, let $\mathrm{A} = \{A_1, A_2, \cdots, A_n\}$ be a sequential mechanism with *n* elements. $A_i (1 \le i \le n)$ satisfies ε_i-differential privacy. Sequential mechanism *A* satisfies $\sum_{i=1}^{n} \varepsilon_i-$ differential privacy.

4. Problem model and Proposed method

In this paper, a novel algorithm, denoted as FIMDP, is designed to obtain *K* itmesets whose support are more than the other itemsets. And FIMDP can guarantee security of sensitive information in frequent itemsets. There are two steps in FIMDP. FIMDP applies exponential mechanism of differential privacy to truncate original transaction dataset in the first step. In the second step, FIMDP applies Laplace mechanism of differential privacy to obtain noise support of all the itemsets. According to noise support, FIMDP can obtain *K* itemsets whose support are more than the other itemsets. The total privacy budget is equal to ε. And the privacy budgets allocated to two steps are equal to ε_1 and ε_2 respectively. All the privacy budget satisfies equation (6) and $\varepsilon_1 = \varepsilon_2$.

$$\varepsilon = \varepsilon_1 + \varepsilon_2 \tag{6}$$

The detail of FIMDP is showed as follows:

In the first step, FIMDP firstly applies apriori algorithm to obtain all the itemsets in which the number of items contained is less than 2. And then FIMDP can obtain the support of these itemsets. Secondly, according to support, FIMDP can obtain support of *K*th frequent itemsets among those itemsets. The support, denoted as σ_k, is used as threshold. Let $L_1 = \{i_{11}, i_{12}, \ldots, i_{1n}\}$ is a set and $i_{1l} \in L_1 (1 \le l \le n)$ is a 1-itemset. The support of $i_{1l} \in L_1 (1 \le l \le n)$ is more than σ_k. $l_{\max}$ is the best high of transaction in the dataset. If the number of items contained in a transaction in dataset is more than $l_{\max}$, FIMDP applies exponential mechanism to truncate the transaction. Let $t_j = \{t_{j1}, t_{j2}, \ldots, t_{js}\} (l_{\max} < s)$ is a transaction in dataset. The number of items contained in t_j is more than $l_{\max}$. So t_j truncates $s - l_{\max}$ items. The possibility of remaining $t_{j,h} (1 \le h \le s)$ satisfies equation (7).

$$\Pr\{t_{ih}\} = \frac{\exp\left(\frac{\varepsilon_{11} \cdot u(t_{ih}, \sigma_k)}{2\Delta u}\right)}{\sum_{r=1}^{s} \exp\left(\frac{\varepsilon_{11} \cdot u(t_{ir}, \sigma_k)}{2\Delta u}\right)} \quad (7)$$

$$u(t_{ir}, \sigma_k) = \sup(t_{ir}) - \sigma_k \quad (8)$$

$\sup(t_{ir})$ is support of item t_{ir}. Δu is total sensitive of function *u*. And for transaction dataset, the most changing of support of item is equal to 1 by adding or deleting one record. So Δu is equal to 1.

In first steps, FIMDP need scan transaction datasets. And FIMDP truncate all the transaction in which the number of items contained is more than σ_k. The dataset truncated by FIMDP is denoted as truncated dataset.

The method of obtaining $l_{\max}$ is motivate from [8]. The distribution of number of items belonging to L_1 and each transaction in dataset, denoted as $Z = \{z_1, z_2, \cdots, z_k\}$. $z_j \ (1 \le j \le k)$ is amount of transactions containing *j* items from L_1. The elements in *Z* are sorted in increasing order. We apply parameter η to determine $l_{\max}$ as follow.

$$\frac{\sum_{i=1}^{l_{\max}} z_i}{|D|} \ge \eta \quad (9)$$

Parameter η equal to 0.85 [8].

In the second step, FIMDP make used of L_2 and truncated dataset to construct FP-Tree. The detail of construct is shown as follow.

1. For a transaction t_j in dataset, items contained in the transaction are sorted in decreasing order of support.
2. If t_j satisfies condition $L_1 \cap t_j \ne \varnothing$, t_j is used to construct FP-Tree. According to Apriori theorem, if an itemset is not frequent, any itemset containing the itemset is not frequent. The support of itemsets in L_1 is more than σ_k. If $L_1 \cap t_j = \varnothing$, any itemset contained in t_j is not belong to the *K* itemsets whose supports are more than the other itemsets.
3. Based on FP-tree, FIMDP mine all the itemsets and applies Laplace mechanism to obtain noise support of these itemsets. According to noise support, FIMDP can obtain *K* itemsets whose support are more than the other itemsets. Finally, FIMDP output those frequent itemsets and noise support corresponding to those itemsets. For given FP-Tree and item *i*, FIMDP can obtain all itemsets containing item i and support of those itemsets. For transaction dataset, the most changing of support of item is equal to 1 by adding or deleting one record. As a consequence, the global sensitivity of quiring support of itemset equal to 1. So, the noise support of an itemset containing item *i* and containing in a branch is obtained as equation (10). The total noise support of the itemset is equal to sum of noise support in all branches.

$$NSup(X) = Sup(X) + Lap\left(\frac{1}{\varepsilon_2}\right) \quad (10)$$

Analysis of security of FIMDP is shown as follow.

FIMDP firstly truncate original transaction dataset. In order to guarantee security of truncation result, FIMDP applies exponential mechanism to guarantee ε_1 – differential privacy. Secondly, FIMDP applies Laplace mechanism to obtain noise support of all the itemsets. And based on noise support, FIMDP can obtain *K* itemsets whose supports are more than the other itemsets. In this step, FIMDP can satisfies ε_2 – differential privacy. As a result, FIMDP satisfies $\varepsilon = \varepsilon_1 + \varepsilon_2$ – differential privacy.

Per noise support, FIMDP can obtain

5. Performance evaluation

We apply two public datasets to verify the efficiency of FIMDP. The first public dataset is retail dataset which is market data in Belgain market. The second public data is muchroom dataset which record information of health [10]. And ACCURACY and Related Error (RE) is applies to evaluate the efficiency of FIMDP.

$$Accuracy = \frac{|U_p \cap U_c|}{K} \times 100\% \quad (11)$$

$$RE = median_{x \in U_p} \frac{|NSup(X) - Sup(X)|}{\sup(X)} \times 100\% \quad (12)$$

U_p is a set of *K* itemsets whose supports are more than the other itemsets. U_c is a set of itemsets output by algorithm. In this paper, two algorithms proposed in [9] and [10] and are denoted as Priv and ODP, respectively. The experimental results are shown from Fig.1 to Fig.4.

Fig.1 and Fig.3 show the changing of ACCURACY with increasing of privacy budget in two datasets. Experiment results show that the value of ACCURACY is increasing with increasing of privacy budget. And FIMDP is better than other algorithms. Fig.2 and Fig.4 show that the changing of RE with increasing of privacy budget. Experiment results show that the value of RE is decreasing with increasing of RE. And FIMDP is better than other algorithms.

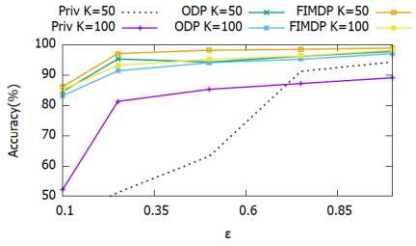


Fig.1 ACCURACY for mushroom dataset

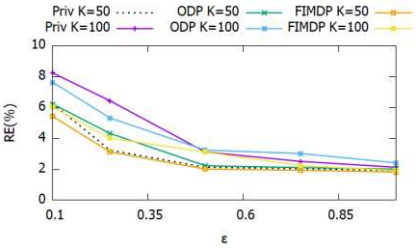


Fig.2 RE for mushroom dataset

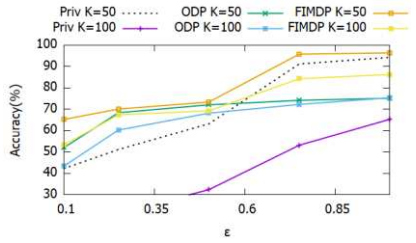


Fig.3 ACCURACY for retail dataset

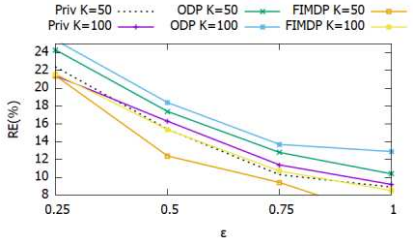


Fig.4 RE for retail dataset.

6. Conclusions

In this paper, we proposed a novel algorithm, denoted as FIMDP. FIMDP can obtain K itemsets whose supports are more than the other itemsets. And FIMDP can guarantee security of frequent itemsets. FIMDP applies exponential Mechanism differential privacy and 1-itemsets to truncate original dataset. And then FIMDP applies FP-tree and Laplace mechanism to noise support of all the itemsets. Finally, according to noise support, FIMDP can obtain *K*itemsets whose supports are more than the other itemsets. In the end, two group experiments are processed to verify efficiency of FIMDP. Experimental results show that the utility of FIMDP is more than traditional algorithms.

Acknowledgements

This paper is supported by Sichuan Science and Technology Program (No. 2019YFG0425, 2019YFG0408); The open Project of Network and Data security Key Laboratory of Sichuan Provence (No. NDS2018-1); the National Natural Science Foundation of China (Grant No.71701026).

References

[1] Haq A U, Li J P, Khan J , et al. Intelligent Machine Learning Approach for Effective Recognition of Diabetes in E-Healthcare Using Clinical Data[J]. Sensors, Vol 20, No. 9, pp. 2649-2654, 2020.

[2] Xu L, Jiang C, Wang J, et al. Information Security in Big Data: Privacy and Data Mining[J]. IEEE Access, vol 2, No. 2, pp. 1149-1176, 2017.

[3] Haq A U, Li J, Ali Z, et al. Recognition of the parkinson's disease using a hybrid feature selection approach[J]. Journal of Intelligent and Fuzzy Systems, Vol 39, No. 1, pp. 1-21, 2020.

[4] Cheng X, Su S, Xu S, et al. DP-Apriori: A differentially private frequent itemset mining algorithm based on transaction splitting[J]. Computers & Security, Vol 50, pp. 74-90, 2015.

[5] H. Zhu, R. Lu, X. Shen, et al. Security in service-oriented vehicular networks[J]. IEEE Wireless Communications, Vol 16, No. 5, pp. 16-22, 2009.

[6] C. Dwork. Differential Privacy[J]. lecture notes in computer science Vol 2, pp. 1-12, 2006.

[7] Apple. Learning with privacy at scale. Machine learning Journal Vol 1, pp. 1-25, 2017.

[8] R. Bhaskar, S. Laxman, A. Simth, et al. Discovering frequent patterns in sensitive data[C]. Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 503-512, 2010.

[9] Li N, Qardaji W, Su D, et al. PrivBasis: Frequent Itemset Mining with Differential Privacy[J]. Proceedings of the VLDB Endowment, Vol 5, No. 11, pp. 1340-1351, 2012.

[10] Zeng C, Naughton J F, Cai J Y. On Differentially Private Frequent Itemset Mining[J]. The VLDB Journal, Vol 6, No. 1, pp. 25-36, 2012.

ELIMINATION OF IRRELEVANT FEATURES AND HEART DISEASE RECOGNITION BY EMPLOYING MACHINE LEARNING ALGORITHMS USING CLINICAL DATA

HUAIYU WEN[1], SUFANG LI[1],AMIN UL HAQ[2], JIAN PING LI[2], RAJESH KUMAR [2],ABDUS SABOOR[2], TAO JIANG[2]

[1]College of Computer Science, Chengdu University, Chengdu, China, 616000
[2]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
E-MAIL: wenhuaiyu@163.com, *khan.amin50@yahoo.com, jpli2222@uestc.edu.cn, rajakumarlohano@gmail.com, sabbor_khan97@yahoo.com, tao1024@yahoo.com

Abstract:

A heart disease diagnosis method has been proposed for effective heart disease diagnosis. In the proposed method Machine Learning (ML) classifiers have been used for detection of heart disease. Chi square feature selection algorithm has been used for related feature selection to improve the prediction performance of machine learning models. Cross validation, method Hold out has been employed for model hyper parameters tuning and best model selection. Furthermore, performance evaluation metrics, such as classification accuracy, specificity, sensitivity, Matthews' correlation coefficient and execution time have been used for model performance evaluation. The Cleveland heart disease data set has been used for testing of the proposed method. The experimental results demonstrated that proposed method has achieved high performance as compared to state of the art methods. Furthermore, the proposed method performance has been compared with deep learning model. Thus, the proposed method will support the medical professional to diagnosis heart disease efficiently and could easily incorporated in healthcare for diagnosis of heart disease.

Keywords:

Machine learning algorithms; Heart disease; diagnosis; accuracy; Feature selection

1. Introduction

Heart disease is a great medical issue and numerous people suffered from it around the world [1]. The HD rate in the United States (US) are more [2]. The signs of HD patient contains, rapidity of inhalation, physical body weakness, swollen of feet [3]. The examination procedures that are used to identify HD were very difficult and its resulting difficulty [4]. The diagnosis and treatment of HD is difficult, particularly in the poor countries [5]. The proper diagnosis of the HD can reduced the risk of HD [6]. According to the report of European Society of Cardiology that 26 million children universal were identified with HD [7]. To the identifying HD through invasive based methods are founded on the examination of patient's health history and analysis of related signs by health specialists. These methods are not suitable for HD diagnosis [8].

To solve the problems in invasive based HD method, a non-invasive method base on machine learning and rough set [9, 10] have been designed by experts for HD detection [11]. Cleveland HD dataset is online available on the UCI which was used by many researchers [12, 13].

In [13] recommended a HD detection approach employing logistic regression and SVM and attained high results. In [14] authors developed a method with global evolutionary methods and attained high prediction accuracy. Furthermore, FS method was incorporated for feature selection and the proposed model gained high performance on selected features. Gudadhe et al. [15] used MLP and SVM for HD identification and 80.41% accuracy obtained. Humar ,et al. [16] developed a HD detection method employing Neural Network that integrates a Fuzzy Neural Network and 87.4% accuracy obtained. In [17] Proposed a heart disease method by employing ML algorithms and achieved good performance.

In this study a new HD diagnosis method has been proposed. Feature selection algorithm Chi squared was used for related feature selection to improve the performance of the classifier from Cleveland data. Five machine learning models were used to predict HD. Model evaluation metrics have employed for model evaluation. The performance proposed method was compared to state of the art method.

The major contribution of the proposed study as follow:

1. Chi squared FS algorithm was used for feature selection to increase the prediction accuracy of the classifiers
2. The proposed method achieved high accuracy on selection features set.
3. The proposed method effectively diagnosis of HD and can be easily incorporated in health care.

The paper organization in such a way that I section proposed method methodology has been explained. The experiments and results discussion are being reported in 3 section. In section 4 conclusions and future work are discussed.

2. Materials and method

The data set and background of the proposed has been presented in below sections in details.

2.1. Data Set

The "Cleveland heart disease dataset 2016" has been used by different scholars [13]. This data set On UCI repository is available.

2.2. Feature Selection Based on Chi-squared Algorithm

Chi Squared is FS algorithm and in various research, study used it for FS [27] is algorithm calculates X^2 between each feature and target variable and select the necessary number of features with the best X^2 scores. The foundation is that if a feature is autonomous of the target variable it is uninformative for classifying clarifications. The chi-square is stated mathematically in eq (1).

$$X^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i} \quad (1)$$

Where O_i is the number of interpretations in class and E_i is the number of probable explanations in class i if there is no relation between the feature and target variable.

2.3. Classification models

The following ML algorithms are incorporated in classification process of the proposed method.

2.3.1. Logistic regression

One of the famous ML model is Logistic Regression (LR) [18] and it is incorporated mostly in classification related problems [21, 22, 25, 26]. It is used for binary machine learning problem of classification to predict the value of predictive variable y when y$\in$ {0, 1}.

The LR logistic function can be expressed in eq (2).

$$\mathrm{h}\theta(\mathrm{x}) = \mathbf{g}(\theta^{\mathrm{T}}\mathrm{x}) \quad (2)$$

Where, $\mathbf{g}(\mathbf{z}) = \frac{\mathbf{1}}{\mathbf{1}+x^{-z}} \mathbf{h\theta}(\mathbf{x}) = \frac{\mathbf{1}}{\mathbf{1}+x^{-z}}$

The Objective function of LR expressed mathematically in eq (3).

$$J(\theta) = \frac{1}{m}\sum_{i=1}^{m} Cost(h\,\theta(\,x^{(i)}), y^{(i)}) \quad (3)$$

2.3.2. Decision Tree

Decision Tree is machine learning model [19] and used for problems of classification [20, 21]. Tree models split the dataset numerous epochs according to definite features limit values. Over piercing, various subclasses of the data-set are design, with each sample fitting to one sub-set. The last sub-sets are terminal (leaf) nodes while the in-between sub-sets are interior nodes. To guess the outcome in each terminal node, the systematic outcome of the training-data in this node is incorporated.

2.3.3. Support Vector Machine (SVM)

For binary classification related problem SVM is usually employed [23, 24]. In the situation of binary combination, the instances are divided by a hyper-plane $w^T x + b = 0$, and w and d-dimensional co-efficient vectors, which is group for the external hyper-plane. The b, are offset from the origin, x is values of the data-set. SVM gets w and b outcomes. The w can resolve in the linear circumstance by calculation Lagrangian multipliers. The w result written as w=, $\sum_{i=1}^{n} \alpha_i y_i x_i$, the n is the number of supported vectors, yi is the output target labels cross ponding to x. The w and b are calculated as written in eq (3). The linear- discriminating function written in eq (4).

$$g(x) = \text{sgn}\,(\sum_{i=1}^{n} \alpha_i y_i\, x_i^T x + b\,) \quad (4)$$

The nonlinear setup expressed in eq (5) for Kernel Trick (KT) and Decision Function.

$$\mathrm{g(x)} = \text{sgn}\,(\sum_{i=1}^{n} \alpha_i y_i K(x_i, x) + \mathrm{b}\,) \quad (5)$$

The Positive Semidefinite Functions (PSF) that follow Mercer's condition as Kernel Functions (KF) [8].

2.3.4. Naïve Bayes (NB)

The NB is ML algorithm and employing mostly for problems of classification [28, 29].

and it is built on a constrained probability statement to state the class of a new vector of features. The NB procedures

the training data to find out the restricted possibility charge of vectors for a specified class.

2.4. Hold out cross validation

The hold out cross validation method has been for training and validation of the model. According to hold out CV 70% of the data used for training and 30% for validation of the model.

2.5. Performance evaluation metrics

Performance evaluation metrics were used for model performance evaluation. These metrics are computed with the help of the confusion matrix. Table 1 shows the binary classification matrix.

Table 1 Confusion matrix [30, 31, 32]

	Predicted Absence of HD subject (0)	Predicted presence of HD subject (1)
Actual Healthy Subject 0	TN	FP
Actual HD Subject 1	FN	TP

From Table 1 we computed the following performance evaluation metrics and mathematically shown in eqs (6), (7), (8), (9), (11), and (11) respectively.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \text{x}100\% \quad (6)$$

$$\text{Sensitivity} = \frac{TP}{TP+FN} \text{x}100\% \quad (7)$$

$$\text{Specificity} = \frac{TN}{TN+FP} \text{x}100\% \quad (8)$$

$$\text{Precision} = \frac{Tp}{Tp+FP} \text{x}100\% \quad (9)$$

$$\text{MCC} = \frac{TP \times TN - FP \times FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \text{x}100\% \quad (10)$$

$$F1 - score = 2 . \frac{\text{precision.recall}}{\text{precision+recall}} \quad (11)$$

2.6. Proposed classification method for heart disease

In the proposed method of heart disease identification, the Cleveland heart disease data set was preprocess in order to normalized data set, Chi squared FS method was used for feature selection and then these features were used for training and testing of the models. Hold out cross validation method was used for training and testing of the models. Furthermore, performance evaluation metrics were used for model evaluation of performance. The pseudocode of the proposed method has been given in algorithm1. The proposed method Flow chart has been given in Figure 1.

Alg.1 pseudocode of proposed HD diagnosis method

Begin

Step1: The HD dataset using pre-processing methods;

Step2: Features selection using Chi squared;

Step3: Hold out method was used for model training and testing

Step4: Metrics of performance evaluation were computed for model evaluation;

Step5: Finish;

End

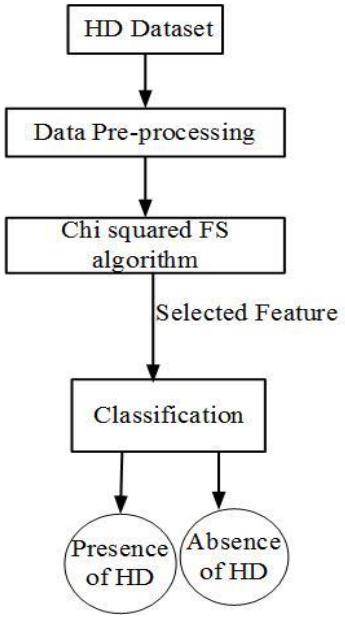


Fig.1 Flow chart of proposed HD method Experimental results and discussion

3. Experimental results and discussion

Different experiment has been performed in order to test the proposed method. Cleveland heart disease data set has been used in our experiments for testing of the proposed method. Chi squared algorithm has been used for feature selection and on these features set the classifiers have been trained and tested. Hold out cross validation method was used for models validation. Different performance evaluation metrics have computed for models perfo4mance evaluation. For simulation python programming language has been used on Intel(R) CoreTM i5-2400CPU @3.10 GHz PC window 10 with different machine learning libraries. All

experimental results have been reported in tables and graphically demonstrated for better understanding.

3.1. Pre-processing of data set

The data set has been preprocess using preprocessing techniques in order to normalized. After preprocessing the data set has 297 instances with 13 features. The process data set has been used for all experiments.

Figure 3. Histogram of data set

3.2. Feature selection by Chi squared FS algorithm

After the data preprocessing, feature selection process has been performed by using Chi squared feature selection algorithm. The feature selected by Chi squared algorithm has been reported in Table 2. According to Table 2 these are important features in the prediction of HD. These selected features have been used for training and testing of the ML models. These have been labeled and the weight of these features have been shown in Table 2. The selected features by Chi square algorithm have been graphically shown in Figure 2 for better understanding.

Table 2 Features selected by Chi squared FS algorithm

S.no	Feature name	Feature code	weight
1	Sex	SEX	0.523
2	Chest pain	CPT	0.217
3	Resting blood pressure	RBP	0.165
4	Serum cholesterol	SCH	0.575
5	Resting electrocardiographic	RES	0.696
6	Maximum heart rate	MHR	0.123
7	Exercise induced angina	EIA	0.298
8	Old peak	OPK	0.561
9	ST	PES	0.574
10	vessels	VCA	0.140
11	Thallium scan	THA	0.486

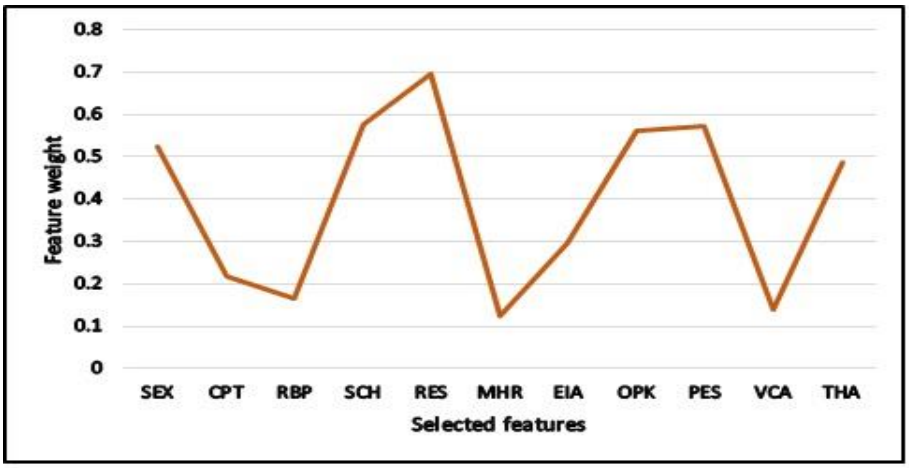


Fig.2 Feature selected by Chi squared FS algorithm

3.3. Classification results of machine learning classifiers on Full features set

The classification performance of machine learning models such as logistic regression, decision tree, support vector machine and Naïve Bayes have checked on full features set along with essential parameters of these model. All models have been trained with 70% of the data and validation with 30%. The experimental results of all models has been reported in Table 3. According to Table 3 the classifier LR achieved 85% accuracy, 87% specificity, 90% sensitivity, 86% MCC, 86% F1-score and computation of model was 0.003 seconds. DT classifier obtained these results on full features set 54% accuracy, 99% specificity, 76% sensitivity, 88% MCC, 87% F1-score and computation of model was 1.241 seconds. The classifier SVM with linear model under the hyper parameters C=1 and γ=0.001 classification results achieved on full feature set were set 86% accuracy, 89% specificity, 86% sensitivity, 87% MCC, 88% F1-score and computation of model was 1.221 seconds. Similarly, NB classification on full feature were 76% accuracy, 87% specificity, 88% sensitivity, 85% MCC, 77% F1-score and computation of model was 6.123 seconds.

The performance of SVM inn term of accuracy was high as compared to other models with full features set. The Figure 3 show the classification performance of these

model with full features set. The computation of these models with full feature s set has been shown in Figure 4 for better understanding.

The computation of LR is low as compared to other models.

Table 3 Performance of models with full features set

Model	Parameter	Performances metrics					
		Acc(%)	Sp(%)	Sn(%)	MCC(%)	F1-Score(%)	Time(%)
LR	C=1	85	87	90	86	86	0.003
DT	-	54	99	76	88	87	1.241
SVM	C=1, γ=0.001	86	89	86	87	88	1.221
NB	-	76	87	88	85	77	6.123

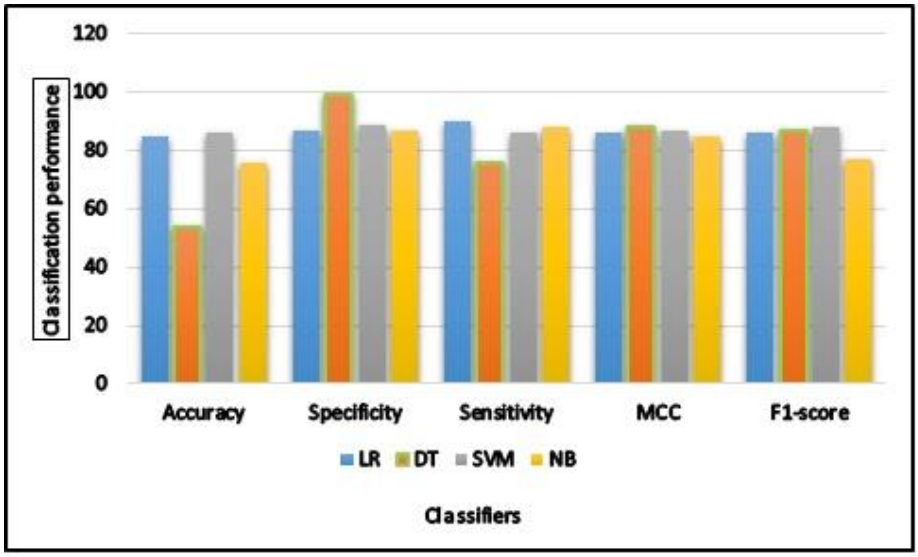


Fig.3 Classifier performance on full features set

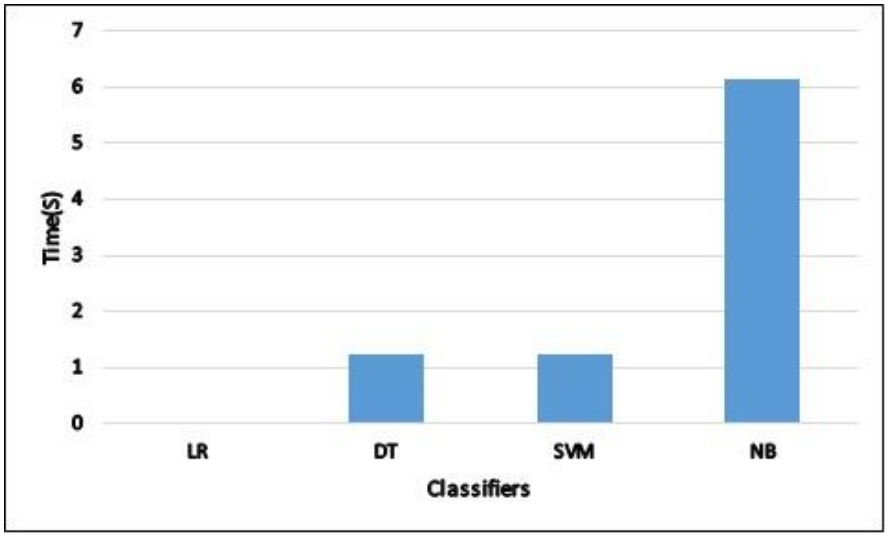


Fig.4 Processing time od models with full features set

3.4. Classification results of machine learning classifiers on Selected features set

The classification performance of machine learning models such as logistic regression, decision tree, support vector machine and Naïve Bayes have checked on selected features set along with essential parameters of these model. All models have been trained with 70% of the data and validation with 30%. The experimental results of all models has been reported in Table 4. According to Table 4 the classifier LR achieved 90% accuracy, 89% specificity, 99% sensitivity, 89% MCC, 90% F1-score and computation of model was 0.002 seconds. DT classifier obtained these results on selected features set 67% accuracy, 99% specificity, 88% sensitivity, 89% MCC, 67% F1-score and computation of model was 0.031seconds. The classifier SVM with linear model under the hyper parameters C=1 and γ=0.001 classification results achieved on selected feature set were set 93% accuracy, 99% specificity, 90% sensitivity, 90% MCC, 92% F1-score and computation of model was 0.021 seconds. Similarly, NB classification on selected feature were 78% accuracy, 80% specificity, 98% sensitivity, 89% MCC, 79% F1-score and computation of model was 2.120 seconds.

The performance of SVM inn term of accuracy was high as compared to other models on selected features set. The Figure 5 show the classification performance of these model with on selected features set. The computation of these models with selected feature s set has been shown in Figure 6 for better understanding. The computation of LR is low as compared to other models.

The best classifier SVM performance on full and selected features set has been shown in figure 7 in term of accuracy and in figure 8 in term of processing time for better understanding. According Figure 7 and 8 the classifier SVM obtained high results on selected features set as selected by Chi square FS algorithm.

Thus, features selection have important rolls in classification problem. On selected features the model performance greatly improved and computation time decreased greatly.

Table 4 Models performance on selected features set

Model	parameter	Performances metrics					
		Acc(%)	Sp(%)	Sn(%)	MCC(%)	F1-Score(%)	Time(%)
LR	C=1	90	89	99	89	90	0.002
DT	-	67	99	88	89	67	0.031
SVM	C=1, γ=0.001	93	99	90	90	92	0.021
NB	-	78	80	98	89	79	2.120

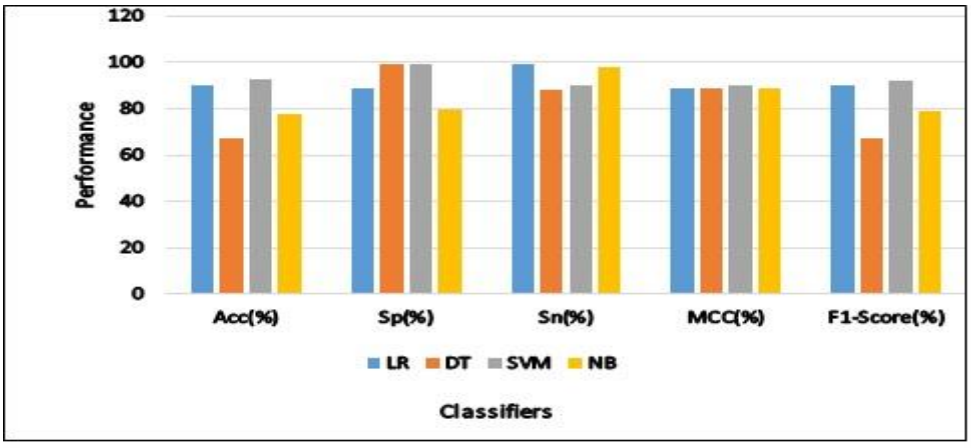


Fig.5 Models performance on selected features set

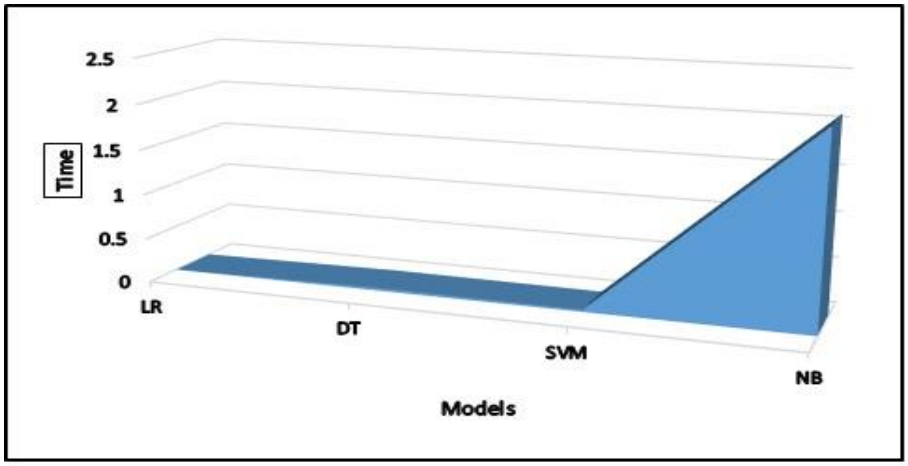


Fig.6 Processing time of models on selected features set

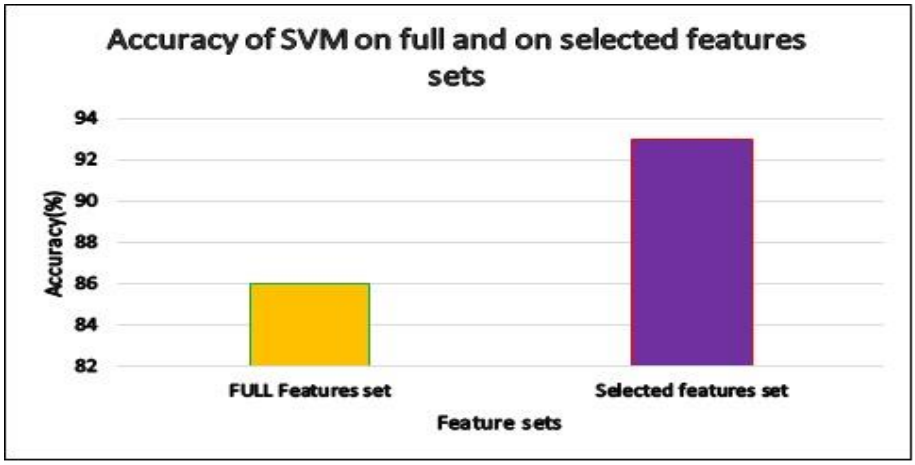


Fig.7 Accuracy of SVM on Full and on selected features sets

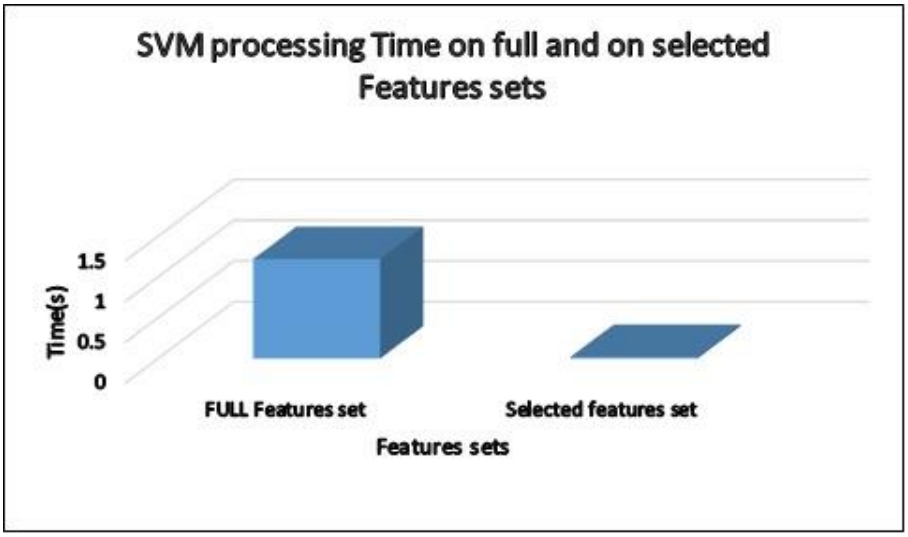


Fig.8 Accuracy of SVM on Full and on selected features sets

3.5. Deep learning model for HD detection

We also use deep learning model for detection of HD using full set of feature. The deep learning model with essential parameters has been trained and tested and reported in Table 5. Deep learning architecture such as DNN1, DNN2, DNN3, DNN4 have been shown in Table 5. According to Table 5 DNN3 achieved high accuracy 91.10 % as compared DNN1, DNN2, and DNN4.

Thus, according to Table 4 and 5 the classification performance of ML learning model is high as compared to deep learning model. ML learning algorithms need features selection for improving accuracy while deep learning automatically select important features from the data set. The performance of deep learning model on this data set is low because the data set instances are small and deep learning need big data set for deep learning, that why the prediction performance of deep learning on this data set is low. The performance of deep learning model shown in figure 9.

Table 5 Deep learning model for classification of HD

Network	Training instance	Testing instance	Learning rate	Activation function	Epochs	Timing of Training(s)	Prediction accuracy(%)
DNN1	210	87	0.0001	RELU	300	120	89.13
DNN2	210	87	0.0010	RELU	600	130	90.12
DNN3	210	87	0.0011	RELU	800	150	91.10
DNN4	210	87	0.0010	RELU	900	170	90.70

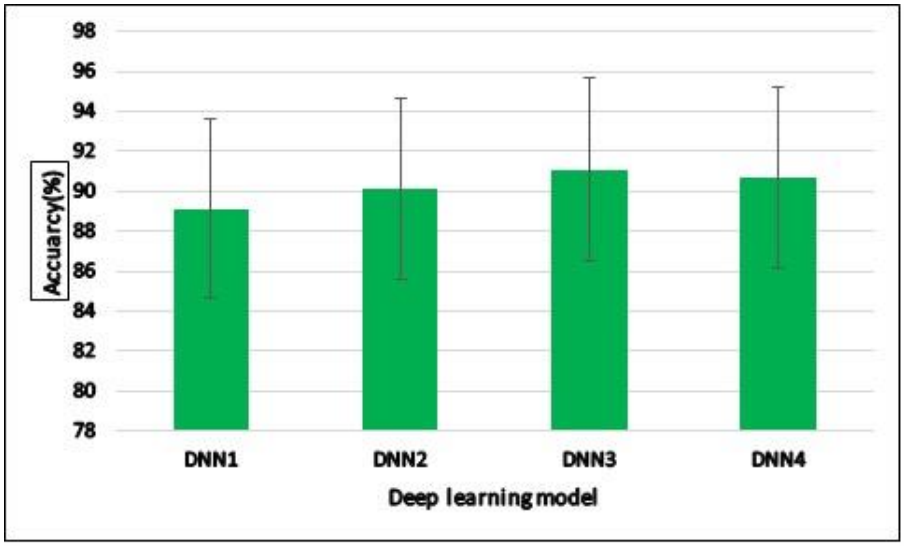


Fig.9 Deep learning performance

3.6. Proposed method performance comparison with existing state of the art methods

The performance proposed method (Chi-squared-SVM) have been compared with state of the art method in Table 6. According to Table 6 the proposed method of HD diagnosis performance was good as compared to existing methods of HD. The Figure 10 show the comparison of accuracy of the proposed method and existing diagnosis methods of HD.

Table 6 Accuracy comparison of proposed method and state of the art methods

Ref	Method	Accuracy(%)
[17]	ANN	88.12
[15]	MLP and SVM	80.41
[32]	Hybrid method	92
[33]	SBF-K-NN	90
Proposed method	Chi-square-SVM	93

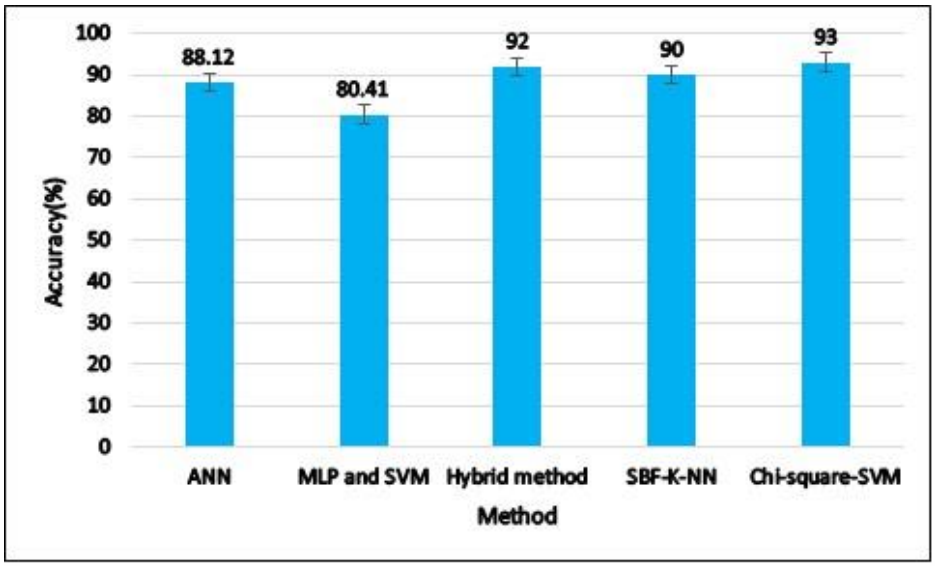


Fig.10 Comparison of accuracy of proposed method and state of the art methods

4. Conclusion

In this research study we proposed heart disease recognition method (Chi-Square-SVM) for efficient detection of heart disease. In the proposed method machine learning models were used for classification of healthy and heart disease subjected rom cleaved data set. We proposed Chi square algorithm for related features selection to improve the classification performance of the models. The experimental results demonstrated that proposed (Chi-Square-SVM) method performance was excellent in term of accuracy and achieved 93% accuracy. Furthermore, performance of proposed method is high as compared deep learning model. The proposed method performance is good as compared to existing heart disease diagnosis methods. The proposed method can easily have incorporated in health care for heart disease identification.

The novelty of the proposed method described as firstly, Chi square feature selection algorithm proposed for related features selection and the features selected by proposed FS algorithm the classifier SVM achieved high accuracy.

Secondly, the performance of SVM is more high as compared to other ML models, so SVM is suitable classifier for HD detection using Cleveland HD dataset. Lastly, the features have low impact in detection of HD are successfully discarded by proposed FS algorithm.

In future, we will use more feature selection and optimization techniques to select more important features from data set to further improve the prediction accuracy of the HD diagnosis system. The proposed method will also apply on other diseases data sets from their detection, such as breast cancer, Parkinson disease. The proposed technique will also deeply on animal and plant disease detection.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province.

Availability of data and materials

The dataset used in this research work available on UCI machine learning repository.

Competing interests

The authors declare that they have no competing interests

Consent for publication

Not applicable.

Ethics approval and consent to participate

Not applicable.

References

[1] A. L. Bui, *et al.*, "Epidemiology and risk profile of heart failure " *Nature Reviews Cardiology,* vol. 8, pp. 30-41, 9,November 2011.

[2] P. A. Heidenreich, et al., "Forecasting the Future of Cardiovascular Disease in the United States:A Policy Statement From the American Heart Association," Journals - American Heart Association, pp. 933-944, 1, March 2011.

[3] M. Durairaj and N. Ramasamy, "A Comparison of the Perceptive Approaches for Preprocessing the Data Set for Predicting Fertility Success Rate," International Journal of Control theory and Applications, vol. 9, pp. 256-260, 2016.

[4] B. A. Mourão-Miranda J1, Born C, Hampel H, Stetter M., "Classifying brain states and determining the discriminating activation patterns: Support Vector Machine on functional MRI data.," Elsevier, vol. 28, pp. 980-995, 4,November 2005.

[5] S. Ghwanmeh, et al., "Innovative artificial neural networks-based decision support system for heart diseases diagnosis," Journal of Intelligent Learning Systems and Applications, vol. 5, pp. 176-183, 29, August 2013.

[6] Q. K. Al-Shayea, "Artificial neural networks in medical diagnosis," International Journal of Computer Science Issues, vol. 8, pp. 150-154, March 2011.

[7] J. López-Sendón, "The heart failure epidemic," Medicographia, vol. 33, pp. 363-369, 2011.

[8] V. K and J. Singaraju, "Decision support system for congenital heart disease diagnosis based on signs and symptoms using neural networks," International Journal of Computer Applications vol. 19, pp. 6-12, ,April 2011.

[9] S. Nazir, et al., "Fuzzy logic based decision support system for component security evaluation," Int Arab J Inf Technol, vol. 15, pp. 1-9, 29,Noverner 2015.

[10] S. Nazir, et al., "Birthmark-based software classification using rough sets," Arabian Journal for Science and Engineering, vol. 42, pp. 859-871, 1, December 2017.

[11] A. Methaila, et al., "Early heart disease prediction using data mining techniques " Computer Science

& Information Technology Journal, vol. 24, pp. 53-59, 2014.
[12] O. W. Samuel, et al., "An integrated decision support system based on ANN and Fuzzy_AHP for heart failure risk prediction," Expert systems with applications ElSEIER, vol. 68, pp. 163-172, 13,october 2017.
[13] R. Detrano, "International Application of a New Probability Algorithm for the Diagnosis of Coronary Artery Disease," American Journal of Cardiology, vol. 64, pp. 304-310, 1989.
[14] B. Edmonds, "Using Localised 'Gossip'to Structure Distributed Learning," 2005, pp. 1-12.
[15] M. Gudadhe, et al., "Decision Support System for Heart Disease based on Support Vector Machine and Artificial Neural Network," in Computer and Communication Technology (ICCCT), International Conference 2010, pp. 741-745.
[16] H. Kahramanli and N. Allahverdi, "Design of a hybrid system for the diabetes and heart diseases," Expert systems with applications, vol. 35, pp. 82-89, 2008.
[17] S. Palaniappan and R. Awang, "Intelligent heart disease prediction system using data mining techniques," in Computer Systems and Applications, 2008. AICCSA 2008. IEEE/ACS International Conference on, 2008, pp. 108-115.
[18] X. Wu, et al., "Top 10 algorithms in data mining," Springer, pp. 1-37, 4,December 2007.
[19] F. E. Harrell and J. (auth.), "Ordinal logistic regression," in Regression modeling strategies, ed: Springer, 2015, pp. 311-325.
[20] K. Lawen, et al., "Interpreting parameters in the logistic regression model with random effects", Biometrics, vol. 56, pp. 909-914, September 2000.
[21] Amin Ul Haq Jian Ping Li Muhammad Hammad Memon Shah Nazir and Ruinan Sun , "A Hybrid Intelligent System Framework for the Prediction of Heart Disease Using Machine Learning Algorithms", Hindawi Mobile Information Systems, Volume 2018, Article ID 3860146, 21 pages https://doi.org/10.1155/2018/3860146.
[22] Amin Ul Haq et.al, Comparative Analysis of the Classification Performance of Machine Learning Classifiers and Deep Neural Network Classifier for Prediction of Parkinson Disease, IEEE, 2018 15th International computer Conference on Wavelet Active Media Technology and Information Processing(ICCWAMTIP), IEEE,14-16 Dec 2018.
[23] C.-C. Chang and C.-J. Lin, "LIBSVM: a library for support vector machines," ACM transactions on intelligent systems and technology (TIST), vol. 2, p. 27, 2011.
[24] H.-L. Chen, et al., "A support vector machine classifier with rough set-based feature selection for breast cancer diagnosis," Expert systems with applications, vol. 38, pp. 9014-9022, 2011.
[25] Amin Ul Haq, Jian Ping Li , Muhammad Hammad Memon, Shah Nazir et al. Feature Selection Based on L1- Norm Support Vector Machine and Effective Recognition System for Parkinson's Disease Using Voice Recordings, IEEE access, April 2019.
[26] https://doi.org/10.1155/2019/5176705
[27] H. Liu, R. Setiono. Chi2: Feature selection and discretization of numeric attributes, Proceedings of 7th IEEE International Conference on Tools with Artificial Intelligence, Herndon, VA, USA, USA, 1995, 388–391
[28] N. Friedman, D. Geiger, M. Goldszmidt. Bayesian network classifiers [J]. Machine learning, 1997, 29(2–3):131–163..
[29] Amin ul haq et al. Heart Disease Identification Method Using Machine Learning classification in E-Healthcare ieee access, 2020, 14
[30] Amin Ul Haq, et al. "A novel integrated diagnosis method for breast cancer detection." Journal of Intelligent & Fuzzy Systems Preprint: 1-16
[31] Amin Ul Haq, et al. "Recognition of the parkinson's disease using a hybrid feature selection approach." Journal of Intelligent & Fuzzy Systems Preprint: 1-21.
[32] Amin Ul Haq, et al. "Intelligent Machine Learning Approach for Effective Recognition of Diabetes in E-Healthcare Using Clinical Data." Sensors 20.9 (2020): 2649.
[33] A. U. Haq, J. Li, M. H. Memon, M. Hunain Memon, J. Khan and S. M. Marium, "Heart Disease Prediction System Using Model Of Machine Learning and Sequential Backward Selection Algorithm for Features Selection," 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), Bombay, India, 2019, pp. 1-4, doi: 10.1109/I2CT45611.2019.9033683.

BREAST CANCER DIAGNOSIS USING DIGITIZED IMAGES OF FNA BREAST BIOPSY AND OPTIMIZED NEUROFUZZY SYSTEM

JALALUDDIN KHAN[1*], NOORBAKHSH AMIRI GOLILARZ[1*], JIAN PING LI[1*], PAIDAR KUZELI[2], ABDOLJALIL ADDEH[3], AMIN UL HAQ[1]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China
[2]Department of Computer Engineering, Amirkabir University of Technology, Tehran, Iran
[3]Faculty of Electrical and Computer Engineering, Babol Noshirvani University of Technology, Babol, Iran
E-MAIL: jalal4amu@yahoo.com, noorbakhsh.amiri@std.uestc.edu.cn, jpli2222@uestc.edu.cn, paidar.kozehli@gmail.com, jalil_addeh@yahoo.com

Abstract:

Breast cancer is the second highest cause of cancer death among women all around the world, especially between the ages of 40 and 65. Early detection of breast cancer tumor type, benign or malignant, has remained a big challenge for physicians and radiologists. By timely identifying the tumor and knowing its type, it can allow physicians to conduct the treatment in the right direction and to take appropriate medications for that type of tumor. Therefore, it is highly important to know the type of tumor accurately to save the patient's life. This paper proposes an intelligent diagnosis method for breast cancer tumor type detection and classification based on fine needle aspirate (FNA) of a breast mass and optimized fuzzy sets. The developed method applied image processing and feature selection techniques to analyze the digitized image of a FNA. In the developed method, nine features computed from a digitized image of a FNA of a breast mass are uses as the initial input of neuro-fuzzy system. In the proposed method, we applied the Association Rules (AR) to find the most informative and effective features of the extracted features. Moreover, in order to advance the act of neuro-fuzzy system, Chaotic Bat Optimization Algorithm (CBOA) is used as learning algorithm. The proposed method is tested on Breast Cancer Wisconsin (Diagnostic) data set. The obtained numerical analysis showed that the developed diagnostic system has excellent performance and high degree of precision.

Keywords:

ANFIS; Breast cancer; FNA; Training algorithm; Tumor type

1. Introduction

Breast cancer is the widespread form of cancer throughout the world and the second most common reason of deaths due to cancers in females, especially between ages of 40 and 65. All women, regardless of genetic or environmental issues, are at threat for breast cancer and its deadly consequences [1]. If a woman reaches the age of 85, she has been at a 12% chance (one in eight) of developing breast cancer at some point in her lifetime [2]. Considering the certain reasons of this disease still remain unidentified for doctors and researchers, early diagnosis and detection of sarcoma is the main step to reduce the rate of death among women. Early detection needs an accurate and reliable diagnosis methods that should be able to distinguish malignant and benign tumors with high accuracy [3].

Fine needle aspiration (FNA) is an effective and simple approach that is done with a tiny needle (about 20- 24 gauge) to acquire samples of fluid and breast tissue. The FNA is the most popular and practical method among doctors and radiologists for identification of breast cancer tumor existence. However, it is not perfect and has its some drawbacks. It is still a big challenge for radiologists to differentiate between malignant and benign tumors using digitized FNA images with confidence. Clearly, this approach suffers from the human mistakes and error with visual inspection, which may further be reinforced by low-quality of the FNA recorded digitized images [3].

Based on the researches in relation to breast cancer tumor type identification and classification, there exist number of essential matters in the design of automatic breast cancer detection system that if suitably handled, increase the effectiveness of classification system. Selecting the most effective and informative attribute subset from raw dataset is one of these essential and important issues. Most of the previous approaches have used the unprocessed data (all attributes obtained from digitized FNA images) as the inputs of classifier. Ineffective and unnecessary attributes expand the size of the search area and lower the detection accuracy. Therefor in the proposed method, association rules (AR)

technique is used to select the all the better attributes and reduce the input vector dimension.

The second topic is related to classifier class and its capability in dealing with complicated pattern recognition tasks like this problem. The proposed method uses neuro-fuzzy system for breast cancer diagnosis. In the developed diagnostic method, adaptive neuro-fuzzy inference system (ANFIS) is implemented. The efficient design of ANFIS-based diagnostic structures prerequisite for truthful training of parameter between its different layers. Standard learning algorithm of ANFIS is hybrid learning algorithm constituted of back propagation (BP) and least squares (LS) named method BP-LS algorithm. The review of previous studies shows that non-derivative approaches which use meta-heuristic algorithms such as nature-based optimization algorithms are more efficient in ANFIS training and tuning [4]. In this study, we have proposed chaotic bat optimization algorithm (CBOA) to train the ANFIS optimally in order to increase its accuracy. In recent years, nature-based optimization algorithms, neural networks and thresholding have been applied in various problems [5- 17].

2. Proposed method

This article suggests a new automatic and accurate diagnosis method for breast cancer tumor type detection and classification. The diagnosis approach includes three main parts including attribute selecting part, classifying part and non-derivative learning algorithm part. The general steps of the proposed diagnosis approach for breast cancer is shown by Figure 1.

Fig.1 Main steps of the proposed diagnosis method

In the first part, association rule method is utilized in order to select the best attributes. This task will minimize the number of features in the input vector. This attribute selection technique finds intriguing associations within numerous group of items [18]. Lowering of input size and selecting the informative and illuminating attributes will enhance the classification accuracy significantly and decrease the computation burden for the classifier in the next step.

In training of neuro-fuzzy system or any ML algorithm, weights are computed based on the input-output pairs and preferred learning algorithm and. The type of learning algorithm and its efficiency is a critical issue in designing of ANFIS. Considering that derivative-based approaches fall over sectional minimum, in the proposed method we have proposed the application of CBOA as the effective and accurate learning algorithm. Figure 2 shows the main parameters in structure of fuzzy system, antecedent and conclusion parameters, that should be determined. Therefore, a set of antecedent and conclusion parameters of ANFIS correspond to an optimal target or food source in CBOA. In the proposed method we used classification accuracy as fitness function or objective function for optimization algorithm.

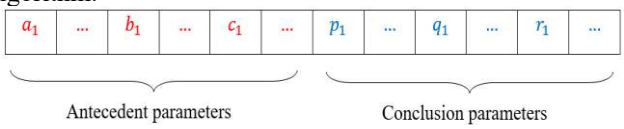


Fig.2 A bat in the proposed method

3. Results

In this section the results obtained through computer simulations of the proposed method are presented with details. Traditional ANFIS with BP-LS learning algorithm is used to compare with CBOA-based ANFIS learning algorithm. The 50% of data is used for training and the remaining 50% is used for testing the trained mode.

3.1. Dataset

The concert of the projected system is evaluated on Breast Cancer Wisconsin (Diagnostic) data set [19]. Researchers have donated the Wisconsin Diagnostic Breast Cancer (WDBC) data set, which have totally 569 instances. Each sample includes 30 features in 10 categories for each cell nucleus, which are extracted from a digitized image of a FNA of a breast mass. More details about WDBC are listed in Table 1.

3.2. Performance on original WDBC

The function of the neuro-fuzzy system using original WDBC data record is studied in this subsection. According to extensive simulations and best results, the input and output variables are considered to be as Gaussian membership function. Antecedent and conclusion parameters are trained based on BP-LS learning algorithm. According to the best obtained results, ANFIS with BP-LS learning algorithm and original WBC data record could classify the specimens by 96.84% accuracy (Table 2).

Table 1 WDBC database

Feature	Range		
	Mean	Standard error	Maximum
Radius ($F_1 - F_3$)	6.9 – 28	0.11 – 2.87	7.93 – 36
Texture ($F_4 - F_6$)	9.7 – 39	0.36 – 4.8	12 – 49.5
Perimeter ($F_7 - F_9$)	43.79 – 188	0.76 – 21.9	50.4 – 251.2
Area ($F_{10} - F_{12}$)	143 – 2501	6.8 – 542.2	185 – 4254
Smoothness ($F_{13} - F_{15}$)	0.053 – 0.16	0.002 – 0.03	0.071 – 0.22
Compactness ($F_{16} - F_{18}$)	0.019 – 0.34	0.002 – 0.13	0.027 – 1.05
Concavity ($F_{19} - F_{21}$)	0.000 – 0.42	0.000 – 0.39	0.000 – 1.25
Concave points ($F_{21} - F_{24}$)	0.000 – 0.2	0.000 – 0.05	0.000 – 0.29
Symmetry ($F_{25} - F_{27}$)	0.106 – 0.3	0.008 – 0.07	0.157 – 0.66
Fractal dimension ($F_{28} - F_{30}$)	0.050 – 0.09	0.001 – 0.03	0.055 – 0.20

Table 2 Performance of ANFIS on original WDBC data record (recognition accuracy = 96.84%)

	Benign cases	Malignant cases
Benign cases	157	4
Malignant cases	5	119

3.3. Performance of ANFIS on after features selection

In the developed diagnostic method, we used AR approach to lower the number of attributes in the input vector. According to AR, 11 of 32 features are removed for WDBC data record. In this state, the input vector has 21 features that are effective collection. The removed features are $F_1, F_4, F_7, F_{11}, F_{14}, F_{17}, F_{18}, F_{21}$, F_{25}, F_{28} and F_{29}. Table 3 shows the performance of different classification approaches. In this state, the BP-LS-ANFIS has ability to classify the inputs with 98.24% precision. The accuracy in the case of using all WDBC attributes (original WDBC data record) was 96.84%, whereas by using only effective features (and cancelling uninformative attributes) the classification accuracy improved remarkably.

Table 3 Performance of traditional fuzzy system on best attributes (RA= 98.21%)

	Benign case	Malignant case
Benign case	159	2
Malignant case	3	121

3.4. Performance of AR-CBOA-ANFIS

In the proposed method, CBOA is utilized as learning algorithm to train the ANFIS efficiently. As mentioned in the above, input and output variables are considered to be as Gaussian membership function. The parameters of Gaussian membership function for the first input (F_1) obtained by conventional learning algorithm BP-LS, and CBOA are listed in Table 4 as an example and shown by Figure 3.

Table 4 Membership function of first input by different BP-LS and CBOA algorithms

Algorithm	LS-BP	CBOA
Membership function 1	{3.41 10.17}	{3.45 10.22}
Membership function 2	{2.92 20.71}	{2.95 20.95}
Membership function 2	{3.53 29.512}	{3.46 29.960}

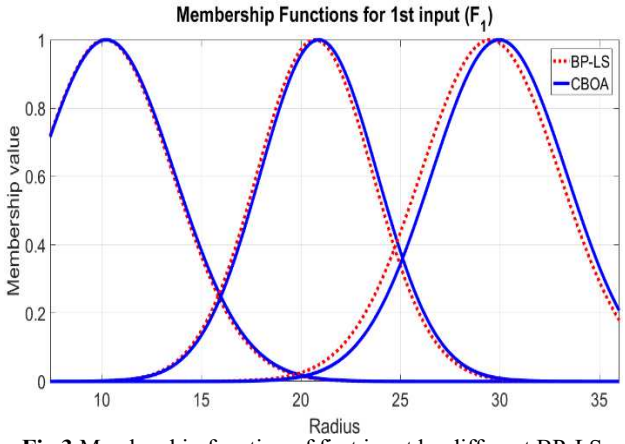


Fig.3 Membership function of first input by different BP-LS and CBOA algorithms

In this case, three membership functions are implemented for each input and 18 fuzzy rules are obtained, and the obtained result are listed in Table 5. It can be seen that different learning algorithms have led to different parameters, which these different parameters lead to different performance.

Table 5 Performance of AR-CBOA-ANFIS (RA= 99.29%)

	Benign case	Malignant case
Benign case	160	1
Malignant case	1	123

In order to comparison the act of AR-CBOA-ANFIS with other breast cancer tumor classification methods, we studied and used some recently introduced method in literature. Table 6 shows the performance of different methods that applied on WDBC. According to the Table 6, the proposed method (AR-CBOA-ANFIS) obtains superior

performance in comparison with other approaches.

Table 6 Comparison with other methods

Ref	Year	Method	RA (%)
[20]	2007	LLS	96.21
[21]	2009	AR+NN	97.32
[22]	2011	AMMLP	99.28
[23]	2012	Support vector machine	98.81
[24]	2012	MLP neural network	95.79
[25]	2013	K-MICA-RBFNN	99.12
[26]	2014	MLP neural network	97.41
[27]	2019	Support vector machine	95.74
[28]	2020		99.71
This study	-	AR-CBOA-ANFIS	99.29

4. Conclusions

In the entire article, an amalgam system constructed on FNA digitized images and ANFIS put forward for classification of tumors in breast. Multiple tests and simulations conducted on WDBC data record to assess and test the performance of the proposed diagnosis method. In the first test, all of the nine attributes of the WDBC data record is used as inputs of the BP-LS-ANFIS. The outcomes of the numerical studies using MATLAB software showed that the BP-LS-ANFIS identifies the breast cancer tumor type with 96.84% accuracy.

In the second experiment, AR attribute selection approach is utilized for effective attribute selection and removal of the superfluous WBC data record attributes. The second and fifth attributes of the WDBC data record are deleted according to AR outcome. In the case of using optimally learned ANFIS and selected features by AR, the developed scheme has ability to classify the input vector (selected WDBC features) with 99.29% precision.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, the project of Science and Technology Department of Chongqing Municipality, Chengdu Chengdian Network Technology Co., Ltd., Chengdu Civil-military Integration Project Management Co., Ltd., and Sichuan Yin Ten Gu Technology Co., Ltd.

References

[1] A. Lewin, L. Moy, P. Baron, and P. Slanetz, “ACR Appropriateness Criteria Stage I Breast Cancer: Initial Workup and Surveillance for Local Recurrence and Distant Metastases in Asymptomatic Women”, Journal of the American College of Radiology, Vol. 16, No. 11, pp. 428-439, 2019.

[2] E. Marrazzo, F. Frusone, F. Milana, A. Sagona, and C. Tinterri, “Mucinous Breast Cancer: A narrative Review of the Literature and a Retrospective Tertiary Single-Centre Analysis”, The Breast, Vol. 5, No. 2, pp. 161-173, 2019.

[3] P. Zarbakhsh, A. Addeh, and H. Demirel, “Early detection of breast cancer using optimized ANFIS and features selection,” 9th International Conference on Computational Intelligence and Communication Networks (CICN), Cyprus, Turkey, Turkey, 2017.

[4] B. Bagheri, H. Peyhani, and M. Akbari, “Financial forecasting using ANFIS networks with Quantum-behaved Particle Swarm Optimization”, Expert Systems with Applications, Vol. 41, No. 14, pp. 6235-6250, 2014.

[5] N. A. Golilarz, H. Gao, W. Ali, and M. Shahid, “Hyper-spectral remote sensing image de-noising with three dimensional wavelet transform utilizing smooth nonlinear soft thresholding function,” in Proc. ICCWAMTIP, Chengdu, China, 2018, pp. 142-146.

[6] N. A. Golilarz, H. Demirel, and H. Gao, “Adaptive generalized Gaussian distribution oriented thresholding function for image de-noising,” International Journal of Advanced Computer Science and Applications, vol. 10, no. 2, pp. 10-15, 2019.

[7] N. A. Golilarz et al., “Optimized wavelet-based satellite image de-noising with multi-population differential evolution-assisted harris hawks optimization algorithm,” IEEE Access, vol. 8, pp. 133076-133085, 2020.

[8] Abdoljalil Addeh, Aminollah Khormali, Noorbakhsh Amiri Golilarz. Control chart pattern recognition using RBF neural network with new training algorithm and practical features. ISA Transactions, 79 (2018) 202-216.

[9] Aminollah Khormali, Jalil Addeh. A novel approach for recognition of control chart patterns: Type-2 fuzzy clustering optimized support vector machine. ISA Transactions, 63 (2016) 256-264.

[10] Hisham Alasmary, Aminollah Khormali, Afsah Anwar, Jeman Park, Jinchun Choi, Ahmed Abusnaina, Amro Awad, DaeHun Nyang, Aziz Mohaisen. Analyzing and detecting emerging internet of things malware: A graph-based approach. IEEE Internet of Things Journal, 6 (2019), 8977-8988.

[11] Milad Salem, Aminollah Khormali, Arash Keshavarzi Arshadi, Julia Webb, Jiann-Shiun Yuan. TranScreen: Transfer Learning on Graph-Based Anti-Cancer Virtual Screening Model. Big Data and Cognitive Computing. 2020, 4(3), 16.

[12] N. Amiri Golilarz, H. Gao, and H. Demirel, "Satellite image De-noising with harris hawks meta heuristic optimization algorithm and improved adaptive generalized Gaussian distribution threshold function," IEEE Access, Vol. 7, pp. 57459–57468, 2019.

[13] N. Amiri Golilarz, A. Addeh, H. Gao, L. Ali, A. Moradkhani Roshandeh, H. Mudassir Munir, and R. U. Khan, "A New Automatic Method for Control Chart Patterns Recognition Based on ConvNet and Harris Hawks Meta Heuristic Optimization Algorithm," IEEE Access, Vol. 7, pp. 149398- 149405, 2019.

[14] M. Shahid et al., "Wavelet Based Image De-noising with Optimized Thresholding Using HHO Algorithm," 16th IEEE International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, pp. 6-12, 2019.

[15] N. Amiri Golilarz, H. Gao, R. Kumar, L. Ali, Y. Fu, C. Li, "Adaptive Wavelet Based MRI Brain Image De-noising," Frontiers in Neuroscience, Vol. 14:728, 2020.

[16] N. A. Golilarz and H. Demirel, "Image de-noising using un-decimated wavelet transform (UWT) with soft thresholding technique," in Proc. CICN, Girne, Cyprus, 2017, pp. 16-19.

[17] A. Jordehi, "Chaotic bat swarm optimisation (CBSO)", Applied Soft Computing, Vol. 26, pp. 523-530, 2015.

[18] R. Agrawal, T. Imielinski, and A. Swami, "Mining association rules between sets of items in large databases", In: Proceedings of the ACM SIGMOD International Conference on Management of Data, Washington, D.C, 1993.

[19] UCI machine learning repository. URL: http://archive. ics. uci. edu/ml /machine-learning-databases/ breast-cancer-wisconsin/.

[20] B. Guijarro, O. Fontenla, B. Perez, and P. Fraguela, "A linear learning method for multilayer perceptrons using leastsquares," Lecture Notes in Computer Science, Vol. 11, pp. 365–74, 2007.

[21] M. Karabatak, and M. Ince, "An expert system for detection of breast cancer based on association rules and neural network", Expert Systems with Applications, Vol. 36, pp. 3465–3469, 2009.

[22] A. Marcano-Cedeno J. Quintanilla-Dominguez, and D. Andina, "WBCD breast cancer database classification applying artificial metaplasticity neural network", Expert Systems with Applications, Vol. 38, pp. 9573–9, 2011.

[23] J. Addeh, and A. Ebrahimzadeh, "Breast Cancer Recognition Using a Novel Hybrid Intelligent Method," Journal of Medical Signals and Sensors, vol. 2, pp. 22-30, 2012.

[24] S. Swathi, S. Rizwana, G. Anjan Babu, P. Santhosh Kumar, and P.V.G.K. Sarma, "Classification of neural network structures for breast cancer diagnosis," Vol. 3, No. 1, pp. 227-231, 2012.

[25] A. Kalteh, P. Zarbakhsh, M. Jirabadi, and J. Addeh, "A research about breast cancer detection using different neural networks and K-MICA algorithm", Journal of Cancer Research and Therapeutics, Vol. 9, pp. 456- 466, 2013.

[26] S. Singh, H. Harini, and B. Surabhi, "An Efficient Neural Network Based System for Diagnosis of Breast Cancer", International Journal of Computer Science and information Technologies, Vol. 71, No. 3, pp. 4354-4360, 2014.

[27] N. Liua, E. Qi, M. Xu, B. Gao, and G. Liu, "A novel intelligent classification model for breast cancer diagnosis", Information Processing and Management, Vol. 56, pp. 609–623, 2019.

[28] A Ul Haq, JP Li, MH Memon, J Khan, S Ud Din, A novel integrated diagnosis method for breast cancer detection, Journal of Intelligent & Fuzzy Systems, 2020.

DYNAMIC FLEXIBLE MULTIPLE-REPLICA PROVABLE DATA POSSESSION IN CLOUD

ZHAO YALING[1], LI SHUQUAN[1]

[1]University of Electronic Science and Technology of China, Chengdu 610000, China
E-MAIL: 201822090534@std.uestc.edu.cn, shuquanli@uestc.edu.cn

Abstract:

With the rapid growth of data and development of cloud storage services, more and more individuals and organizations tend to outsource their data to the cloud environment. Cloud storage brings much convenience to people, but also brings a series of security issues, such as the integrity and reliability of data in the cloud. Based on the characteristics of multi branch tree, a dynamic flexible multiple-replica provable data possession scheme is proposed. The scheme can not only ensure the integrity and reliability of multi ple copies and realized the verification of any number of copies, but also support the dynamic update operation. In addition, the scheme also supports third party audit (TPA) and user privacy protection. The experimental results show that the scheme has high efficiency.

Keywords:

Cloud storage; multiple-replica; data integrity; provable data possession; dynamic;

1. Introduction

With the rapid growth of data and increasing diversification of cloud storage services, the problems in traditional storage systems grow prominent, such as the limited ability of storage and computing in local, the complex management and high cost in maintenance etc. But the cloud service provider (CSP) can solve above problems. It provides users with powerful computing and storage in the form of services, ensure that users can access the data in cloud through the Internet anytime and anywhere, and users only need to pay for CSP according to their actual needs, In order to improve the reliability and availability of data, users often store multiple copies of data in the cloud. However, the CSP is untrusted. Because when users outsource their data to cloud, they will lose direct control of their data. The CSP may claim to store multiple copies, actually only one copy, or even delete files that users rarely used or never used recently to save storage costs. In addition, with the various irresistible factors, the data stored in the cloud may be damaged, and the CSP often hide the corruption or even launch attacks to maintain its reputation. So, the verification for data integrity in the cloud is very important.

To verify the integrity of data stored on the CSP, Ateniese et al. [1] proposed the provable data possession (PDP) scheme for the first time in 2007, but the scheme can only be used in static scenarios. In order to support dynamic operations, Ateniese et al. [2] extended the original scheme to supporting partial dynamic operations in 2008. Then Erway et al. [4] proposed the dynamic data possession provable scheme based on the sorted authentication skip list, which is the first full dynamic PDP scheme, but it increased the communication overhead. In 2011, Wang et al. [3] introduced MHT as the authentication structure to support dynamic operations, but the corresponding communication overhead of the scheme had not been reduced. In 2013, Yang et al. [10] used index table to store changes of data block index, and also gave a verification scheme supporting dynamic operation.

In order to enhance the availability and reliability of multiple copies, a series of schemes for multiple replica integrity verification have been proposed. The MR-PDP scheme proposed by Curtmola et al [5] was the first scheme to verification for multiple copies, but it did not support the dynamic operations. Then Liu et al [6] proposed a scheme used MHT as the structure to support the dynamic operations, but it generated authentication tag for each copy, which increased the calculation cost. In 2015, Zha et al. [13] proposed a scheme based on multi-branch tree (MBT), but the scheme lacked certain flexibility. In 2017, Li et al. [15] proposed a flexible integrity verification scheme, but the scheme did not support the dynamic operations. In this paper, a dynamic and flexible multiple-replica provable data possession scheme is proposed. The scheme supports dynamic operations by introducing multi branch tree, realizes the signature of data by bilinear map, improves the security of data by random mask, and it also supports public verification. The experiments show that this scheme is better than other existing schemes.

2. Preliminary

2.1. Bilinear Map

Let G_1 and G_2 be two multiplicative cyclic groups with the same prime order q, $e: G_1 * G_1 \to G_2$ be a bilinear map, which holds the following properties:

Computable: $\forall u, v \in G_1$, e is calculated effectively Non-degenerate: $\exists u, v \in G_1, e(u, v) \neq 1$
Bilinear: $\forall u, v \in G_1, \forall a, b \in Z_p, e(u^a, v^b) = e(u, v)^{ab}$

2.2. Multi-branch Tree (MBT)

In the MBT, each node has multiple sub nodes, and each leaf node corresponds to a data block. The leaf node value is hash of corresponding data, and the other node value is hash of all its child link form. Figure 1 shows the structure of MBT, as shown in the figure $R_0 = H\big(H(A_1)\|\cdots\|(A_n)\big)$,and $A_1 = H\big(H(m_1)\|\cdots\|H(m_n)\big)$

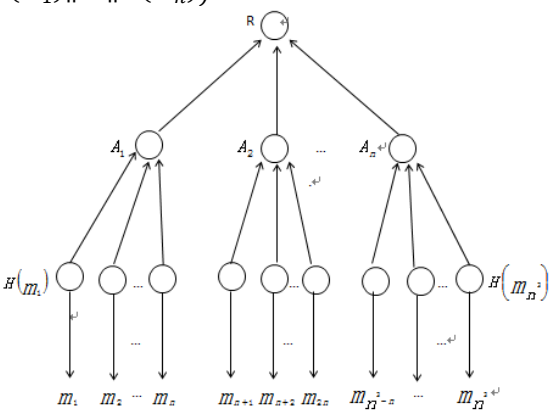


Fig.1 the structure of MBT tree

2.3. System Model

There are three entities in the system:

Data owner (User): users use the services and outsource data to cloud storage.

Cloud service provider (CSP): the cloud storage service provider, with strong computing and storage capabilities, manages and maintains storage devices, and provides services for users.

Third party audit (TPA): the third party audit with strong computing power, users can entrust the TPA to verify data and reduce local burden.

3. Scheme realization

The scheme includes seven algorithms as follows:

(1) $KeyGen() \to (sk, pk, spk, ssk)$:The client performs the algorithm to generate the key. First, the user select random $\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_s \in Z_P$, and defines $v = g^{\alpha_0}$, $g_k = g^{\alpha_k}, (g_k \in G_2)$.So, in this scheme the private key is $sk = \vec{\alpha} = (\alpha_1, \alpha_2, \cdots, \alpha_s)$, the public key is $pk = (g_1, g_2, \cdots, g_s)$ and the MBT signature key is $spk = v, ssk = \alpha_0$ .User saves the sk, ssk locally, the pk and SPK are sent to CSP.

(2) $ReplicaGen(F) \to (F')$: The client performs the algorithm to generate multiple copies $F' = \{m_{i,j}^k\}$,

$$m_{i,j}^k = b_j^k + r_{i,j}^k, r_{i,j}^k = \Psi_{Kr}(i\|j\|k) \quad (1)$$

where $r_{i,j}^k = \Psi_{Kr}(i\|j\|k)$.

(3) $TagGen(F') \to (\Phi)$: The client performs the algorithm to generate tags and the root signature of MBT. The specific operation is as follows:

a) Construct MBT based on hash value for data set and the $\Omega_i (1 \le i \le nm)$.

b) The signature of the MBT root is $T = \big(H(R_0)\big)^{\alpha_0}$,and $R_0 = H\big(H(A_1)\|\cdots\|(A_n)\big)$

c)The block tag is generated from F, that is

$$\sigma_j = \vec{\alpha} \bullet \vec{b_j} = \sum_{i=1}^{s} \alpha_i \, b_j^i, (1 \le j \le m) \quad (2)$$

so, the tag set is $\Phi = \big(\sigma_j\big), (1 \le j \le m)$.

d)The user uploads the data set, tag set, the root signature and the construction information of MBT to the CSP, then deletes the local information.

(4) $ChalGen() \to (chal)$: TPA performs the algorithm to generate challenge. The TPA can determine the number of challenged blocks and replicas randomly. Then TPA sends challenge $chal = \Big(R, \{j, w_j\}_{j \in I}\Big)$ to CSP.

(5) $ProofGen(chal) \to (P)$: After receiving the challenge, CSP performs the algorithm to generate evidence. The CSP calculate μ and σ by the public key, that is

$$\mathrm{u} = \sum_{\mathrm{k}=1}^{\mathrm{s}} \mathrm{g}_{\mathrm{k}}^{\sum_{\mathrm{i} \in \mathrm{R}} \sum_{(\mathrm{i},\mathrm{w}_\mathrm{j}) \in \mathrm{Q}} \mathrm{w}_\mathrm{j} \mathrm{m}_\mathrm{j}^\mathrm{k}} \quad (3)$$

$$\sigma = \sum_{(j,w_j) \in Q} w_j \sigma_j \quad (4)$$

$p = \Big(\mu, \sigma, \{\Omega, H\big(m_{k,j}\big)\} sign_{ssk}\big(H(R_0)\big)\Big)$is sent to TPA.

(6) $Verify(P) \to \{0,1\}$: After receiving the proof, TPA performs the algorithm to verify whether the data is complete. Firstly, the TPA uses $\{\Omega, H\big(m_{k,j}\big)\}$ to calculate the root R_0 and verify whether the equation holds,

$$\mathrm{e}\big(sign_{ssk}\big(H(R_0)\big), g\big) \stackrel{?}{=} \mathrm{e}(H(R_0), v) \quad (5)$$

if the equation is not true, then finished and return 0, else continue to verify whether the equation holds,

$$e(v,g^{\sigma})^{|R|}e\left(v,\prod_{k=1}^{s}g_k^{\Sigma_{i\in R}\Sigma_{(j,w_j)\in Q}w_j r_{i,j}^k}\right)\stackrel{?}{=}e(v,u) \quad (6)$$

if the equation is not true, then finished and return 0, else return 1.

(7) $Dataupdate(b,Id,L)\rightarrow\{0,1\}$: The update includes three operations: modification, insertion and deletion. Users use this algorithm to update the data stored in the cloud. Let us take the modification as the example to explain dynamic operation. Suppose that the user needs to modify the i-th data block:

a) Firstly, user sends an update request to CSP and downloads i-th block data of any copy, then restores the source data $b_i'$and uses decryption algorithm to get original data.

b) Secondly user modifies the data as required, and generates the new source data b_i' ,new tag

$$\sigma_i'=\vec{\alpha}\cdot\vec{b_i}=\sum_{j=1}^{s}\vec{\alpha_j}b_i^j \quad (7)$$

and new data block m_k' ,then sent them to the CSP.

c) After receiving the new data and tag, CSP will update, and generate the auxiliary authentication information Ω_i and hash value $H(m_{k,i}')$ about the corresponding node before updating, then generating new root R_0' , Ω_i' and $H(m_{k,i}')$. Finally, the updated evidence $\{\Omega_i,H(m_{k,i}'),H(m_{k,i}'),\Omega_i'',R_0',T\}$will return to the user.

d) After receiving the evidence, user uses Ω_i' and $H(m_{k,i}')$ to calculates the root $R_0''$and verify whether the

$$e(sign_{ssk}(H(R_0)),g)\stackrel{?}{=}e\left(H\left(R_0''\right),v\right) \quad (8)$$

holds, if it is equal, it means the update position is correct, then uses Ω_i'' and $H(m_{k,i}')$ to calculates the new root $R_0'''$and compares whether the R_0''' and R_0' is equal, if it is equal, the data content is modified successfully, the local tag and data will be deleted ,the new root will be signed $T'=(H(R_0'))^{\alpha_0}$and sent it to CSP. The root signature will be updated after CSP receives it

4. Performance analysis

We take modification as the example for performance analysis. Suppose that user needs to modify t data in the file, and the modification mainly involves the interaction between the CSP and the user. In the MuR-PDP Scheme [12], MHT is used to support the dynamic update, in the data modification phase, the main calculation cost of CSP is $ktT_{hash}+(2kn-1)T_{hash}+kt(T_{hash}+T_{\exp})$, and that of client is $2(2kn-1)T_{hash}+(2kn-1)T_{hash}+2kt(T_{hash}+T_{\exp})+kt(T_{hash}+2T_{\exp}+T_{mul})$; in TB-PMDDP scheme [11], the main calculation cost of CSP is $(2k\log_2(n)+3k)T_{hash}+kT_{hash1}$, and that of client is $t(T_{hash1}+(S_0+1)T_{\exp}+(S_0-1)T_{mul})+(k-1)T_{mul}$; in the scheme [13], the main calculation cost of client and CSP are $kt(T_{hash}+2T_{\exp}+T_{mul})+2kt(2T_{hash}+2T_{\exp})+N_0T_{hash}$ and $2T_{pair}+(kt+1)T_{hash}+N_0T_{hash}$ respectively ; in the proposed scheme, the main computing costs of the client and CSP are $t(S_0T_{mul}+(S_0-1)T_{add})+T_{\exp}+4T_{hash}+2T_{pair}$ and $[k(t+1)+1]T_{hash}$ respectively; assuming the number of copies k = 3, the experimental results are shown as in Figure 2.

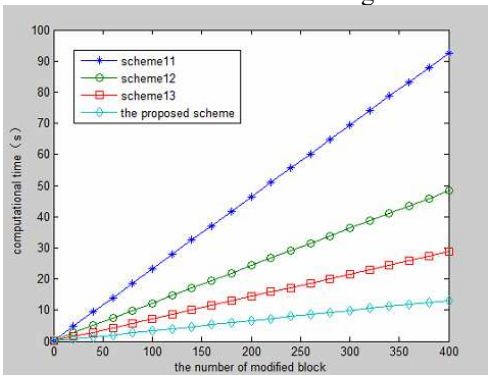


Fig.2 Data Modification

As shown in the figure 2, the calculation cost of the modification increases with the number of data blocks increase, but the experimental results show that the effect of the proposed scheme is better than the other three schemes.

5. Conclusion

In the cloud storage environment, the integrity and reliability of data is a crucial security issue, and the dynamic update is also an indispensable part. The existing schemes mostly use MHT to support dynamic operation, but the structure is very large in the process of verification. In this paper, we use MBT to realize dynamic update and it make the structure of verification is simplified. However, in this scheme, the generation of data copy and tags are completed by user, which makes the calculation pressure of the user greater. How to transfer these calculation processes to CSP safely is the next research direction.

Reference

[1] Ateniese G,Burns R C,Curtmola R,et al.Provable data possession at untrusted stores [C] //Proc of the 14th

AC-M Conference on Computer and Communications Security. New York: ACM Press,2007:598-609.
[2] Ateniese G,Pietro R D,Mancini L,et al.Scalable and efficient provable data possession [C]//Proceedings of 4th International Conference on Security and Privacy in Communications Networks(SecureComm'08). New York, USA:ACMPress,2008:1-10.
[3] Wang Qian,Wang Cong,Ren Kui,et al.Enabling public auditability and data dynamics for storage security in cl-
oud computing [J] . IEEE Trans on Parallel and Distri buted Systems, 2011 ,22 (5):847-859.
[4] Erway C,Alptekin K,Papamanthouc C.Dynamic prova ble data possession [C] //Proc of ACM Co-
nference on C-
omputer and Communications Security.New York : A CM Press ,2009:213-222.
[5] Curtmola R,Khan O,Bums R,et al.MR-
PDP:multiple- replica provable data possession [C] //P roc of the 28th It-
ernational Conferenceon Distributed Computing Syste ms.Piscataway,NJ:IEEE Press,2008:411-420.
[6] Liu Chang,Ranjan R,Yang Chi,et al.MuR -
DPA:top- down levelled multi-
replica Merkle hash tree based secur-
e public auditing for dynamic big data storage on clou d [J] . IEEE Trans on Computers, 2015,64(9):2609-2622.
[7] Wang Cong,Ren Kui,Lou Wenjing,et al.Toward publi c auditable secure cloud data storage servi-
ces [J]. IEEE N-etwork,2010,24(4):19-24.
[8] Zhu Yan,Hu Hongxin,Ahn G J,et al.Efficient audit ser vice outsourcing for data integrity in cloud-
s[J].Journal o-
f System and Software,2012,85 (5):1083-1095
[9] Zhu Yan,Hu Hongxin,Ahn G J,et al.Cooperative prova ble data possession for integrity verificati-
on in multiclo-
ud storage [J].IEEE Trans on Parallel and Distributed Systems,2012, 23 (12):2231-2244.
[10] Yang Kan,Jia Xiaohua.An efficient and secure dynami c auditing protocol for data storage in cl-
oud computing [J].IEEE Trans on Parallel and Distrib uted Systems,2013,24 (9):1717-1726.
[11] Barsoum,A.F.,Hasan,M.A. Provable Multicopy Dynamic Data Possession in Cloud Computing Systems[J].IEEE Transactions on Information Forensics&Security,2017,10(3):485-497.
[12] Liu,C.,Ranjan,R.,Yang,C.,et al.MuR-DPA:Top-Down Levelled Multi-Replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud[J].IEEE Transactions on Computers,2015,64(9):2609-2622.
[13] Zha Yaxing. Reserch of Data Integrity Verification Technology in Cloud Storage Environment[D]. Beijing University of Posts and Telecommunications, 2018
[14] Shacham H,Waters B.Compact proofs of retrievability [C] //Proc of International Conference on the Theory a-
nd Application of Cryptology and Information Securit y.Berlin:Springer,2008:90-107.
[15] LI L,YANNG Y,WU Z.FMR-PDP:Flexible multiple-replica provable data possession in cloud storage[C]//2017 IEEE Symposium on Computers and Communications(ISCC).IEEE.2017:1115- 1121.
[16] Li Mengting, Zhou Anning. Data auditing method based on relative index hash tree in cloud environment [J]. Computer application research, 2019,36 (4): 1148-1152 Anning.Data auditing method based on relative index hash tree in cl-oud environment [J].Application Research of Computers,2019,36(4):1148-1152.
[17] Li Jingwei, Zhu Mingdong. MHT based dynamic data integrity verification and recovery scheme in cloud storage [J].Computer application research,2019,36 (07): 2179-2183 + 2194

DEEP REINFORCEMENT LEARNING FOR COMPUTATION OFFLOADING AND RESOURCE ALLOCATION IN BLOCKCHAIN-BASED MULTI-UAV-ENABLED MOBILE EDGE COMPUTING

ABEGAZ MOHAMMED[1], HAYLA NAHOM[2], AYALL TEWODROS[3], YASIN HABTAMU[4], GEBRYE HAYELOM[5]

[1,2,3,4,5]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China

[1,3]School of Informatics and Computing, Dilla University, Dilla, Ethiopia

E-MAIL: mamsied2002@gmail.com, nahomh185@gmail.com, meettedy2123@gmail.com, habtishyacob@gmail.com, hmuleta@gmail.com

Abstract:

In the current fifth-generation (5G) and Beyond 5G (B5G) era, the Unmanned Aerial Vehicles (UAVs) have been playing a vital role and attracting interest in different application areas in the military, and civil applications such as communications, disaster management, search and rescue, security, control, agriculture, Internet of things (IoT), etc. In these networks, ultra-heterogeneous IoT devices generate time-sensitive traffic. However, those devices have limited resources to compute tasks. Recently, Mobile Edge Computation Offloading (MECO) has been considered as an encouraging model to enable the computation tasks of IoT devices to be performed by MEC servers and support ultra-low latency IoT applications to ensure Quality of services (QoS). However, terrestrial network failure due to natural and human-made disasters has been increasing, and difficult to provide reliable computation offloading and resource allocation services to IoT networks. Nowadays, UAVs have been promising technology to quickly deploy and recover the system to provide efficient services to edge nodes. The offloading and resource allocation problems in current network technology are complex, and offloading task to edge server is vulnerable to security risks. Hence, we utilize a deep reinforcement learning method to handle a complex problem for computation offloading and resource allocations in a dynamic environment. And also, we explore a blockchain-based multi-UAV-assisted MEC architecture in securing and optimizing the offloading problems.

Keywords:

Blockchain; Deep Reinforcement Learning; Massive IoT; Mobile Computation Offloading; Multi-UAV.

1. Introduction

In the past and recent years, cellular technology grows dynamically in different parameters with improvements of latency, energy consumption, and accessing resources in a decentralized way. Several ultra-dense heterogeneous devices from individuals and organizations generate and store large amounts of data via sensors and applications regularly [1]. Nowadays, with the deployment of massive Internet of Things (mIoT) nodes, data produced via sensors increased rapidly from time to time. The dynamic development of mIoT with emerging diverse devices such as wireless sensors, smart machines, and mobile user's applications enables the users to high Quality of Experience (QoE) and Quality of Service (QoS) [2], [3].However, most of these applications are delay-sensitive or real-time applications that need high computational capacity. The edge devices could not compute each task because of their low computation capability and short-life battery; also problematic for edge IoT devices to run these applications [4]. These large data generated by devices need to be stored in a different form of a conventional database system and needs to be processed. In the past decade, the computing task will be transferred and executed in the cloud layer, where the overall computation costs would be high. Some of the IoT sensor's data is required to be processed even faster than the Cloud's present competency. The edge computing technology is a prominent solution that proximate resources to IoT devices at the edge system to balance the gap between edge IoT devices and cloud computing [2].

According to the current cellular networks, Unmanned Aerial Vehicle (UAV) plays an important role where it acts as Aerial Base Station (ABS) to provide services for IoT devices and extend the network coverage.UAVs are predicted to bring new business and research directions for researchers and service providers. In the current and future, millions of UAVs have been used to perform various activities, such as public protection, disaster relief operation, extending the cellular-network coverage in remote area acts

as a flying base station, etc. [5], [6]. In the future of IoT, UAV is a current technology to substitute the coupled sensors at rest with a single device that is deployable to diverse locations, talented of booming flexible payloads, re-programmable, and measuring just about anything, anywhere, and also cost-effective, etc. Recently, Deep Reinforcement Learning (DRL) has been utilized as an evolving tool to solve numerous problems and challenges in today's networks efficiently. It is applicable in Heterogeneous networks (HetNets), IoT, Vehicle to Vehicle (V2V), Machine to Machine (M2M), Vehicle to everything (V2I), Self-Organization cellular networks, and UAV infrastructures become more distributed and autonomous. The works have been realized on machine learning or DRL approach roles for cellular and next-generation wireless networks [7].

The computation offloading process has challenges, such as data integrity violation, data loss during offloading and might not be suitable for the 5G and B5G systems due to the exact central point of service failure [8]. Hence, we propose a blockchain system to solve these problems. Blockchain technology is a digital distributed ledger used in various services to ensure decentralized, immutable, and secure transactions among peer-to-peer nodes; it is ever-growing technology that can assure data completeness. A comprehensive survey presented on the integration of blockchain in IoT networks in different layers [9]. Authors [10] proposed blockchain-based DualFog-IoT architecture to enhance communication systems by reducing resource utilization at the cloud layer.

The contribution of this work outlined as follows:

- We design a new blockchain-based multi-UAV-enabled MEC for IoT network architecture model for resource allocation and computation offloading to secure and keep the QoS and QoE of IoT devices. By adopting blockchain technology, the architecture can identify and prevent IoT devices' malicious behaviors through a trustworthy access control mechanism.
- To obtain optimal offloading policy and allocate resources efficiently by adopting DRL for resource allocation, computation offloading, and energy efficiency, which reduce system costs in A2G network infrastructure.
- Summarizes previous works on the DRL approach for the UAV and the MEC networks are related to our architecture.

The remaining parts of this work are outlined below: Section 2 presents the related works with our proposed architecture from territorial network and aerial network points of view. Our architecture and system model in a multi UAV-enabled edge computing IoT network is proposed in section 3.Finally, section 4 concludes our work.

2. Related works

In recent works have solved complex problems using the DRL approach in edge computing. In software Defined Network(SDN) with the number of virtual networks(VN), [11] proposed a DQN model for energy-efficient resource sharing in green network environments, which consider caching and computation offloading in-network. In [12], the authors have presented a comprehensive survey on DRL based proactive caching and computation offloading in the MEC and IoT network.

The Authors in[13] proposed offloading cellular traffic to WLAN using the DQL algorithm and MDP model to minimize energy consumption and mobile users' cost. The MEC server has limited resources to allocate for all edge devices; thus, the MEC server also minimizes cost and energy. In [14] designed a virtualized computation offloading using DRL and proposed a DDQN-based DQL approach to attain an agent the adequate offloading policy without prior knowledge of the system environment in a dynamic manner.

Furthermore, authors in [15] proposed a trust-based access control mechanism to protect IoT devices against malicious offloading behaviors. Authors [16], also proposed blockchain-based smart contract access control models to provide an adequate protection mechanism for IoT devices by implementing access-right validation. A study in [17] designed smart contracts access management systems for the industrial IoT networks on a blockchain. In [18], it proposed a blockchain-enabled model for access control and authorization of IoT nodes.

UAVs are connected with cellular networks as new user equipment and generate incomes for MEC service providers by computing edge IoT devices' tasks.

Currently, there are many natural disasters such as earthquakes, volcanoes, landslides, and avalanche emergency in the terrestrial network infrastructures where UAVs are network lifesaver, especially in emergency situations[19]. The UAV-assisted emergency network is proposed by Zhao et al.in [20] there placed the destroyed base station by establishing multi-hop D2D users in different cells and relay the signal for emergency communication vehicles. Cellular connected UAVs will be the next generation attractive network that integrates with the future cellular network and ML approach, creating new intelligent aerial mobile users. In [21] proposed a novel framework that deploys an ABS, which assists the overloaded or congested base station in small cells. The previous works used a ML approach that predicts each base station's traffic demand through previous histories to deploy ABS, which serves users in small cells and applies contract theory to moderate each

BS and UAV's utility. Cui et al.[22] studied multi-agent reinforcement learning using Q-learning and stochastic game theory model for dynamic resource allocation in multi-UAV connected with multi-users. Each UAV acts as an agent to independently decide to increase each agent's long-term rewards for reliable communication.

3. System Architecture of Blockchain-based Multi-UAV-enabled Mobile Edge Computing

The A2G network can be integrated with ML algorithms, blockchain, NFV, and SDN to solve complex problems and manage the dynamic network environment. Figures 1 and 2 illustrate the A2G network; access resources from cloud network through Virtualized Base Band Unit (VBBU). In VBBU, the network resources used for A2G network infrastructures are virtualized intelligently. These resources are allocated to the infrastructures depending on the network demands. Figure 2 also shows the multi-UAV-enabled edge computing for IoT networks when the emergency and network traffic exist in different areas. The UAV networks can access resources from the VBB pool and also from satellites to increase network durability.

We categorize the architecture into three layers:

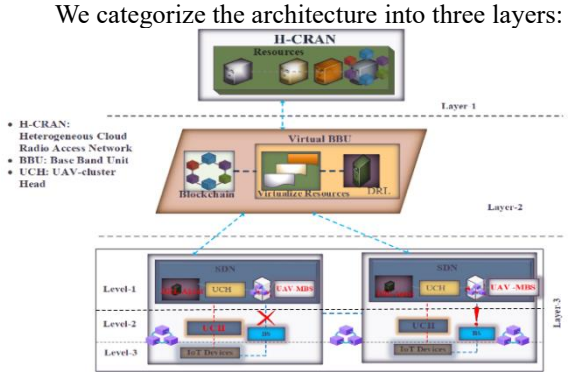


Fig.1 Multi-UAV-enabled edge computing for IoT network in emergency service.

3.1. Layer-1

Heterogeneous Cloud Radio Access Network (H-CRAN) has Cloud computing resources delivered by server-based applications through digital networks or through the public Internet itself. The resources are available on the Cloud far from the edge IoT device. The edge IoT devices need the MEC servers and resource localized to ensure QoS and QoE in the 5G and Beyond network.

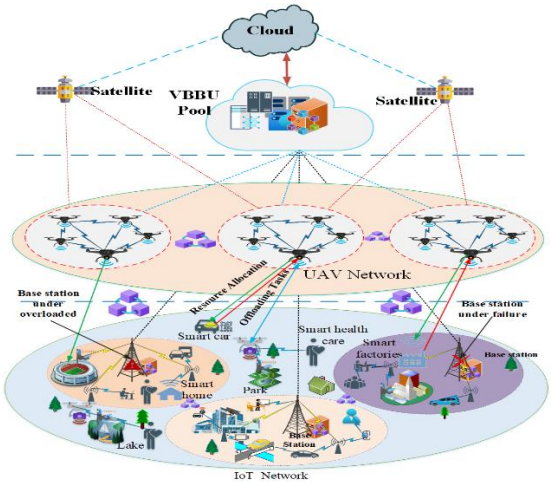


Fig.2 General System model of blockchain-based multi-UAV enabled MEC in three layers.

However, the existing H-CRAN models in 5G have not solved the security challenges such as data availability, privacy, and data integrity. The dynamic data processing in the A2G network environment, information exchange, and resource allocation between a different computational node and IoT devices are vulnerable to third-party attacks. The data transmission between various entities can also be unauthorized and loos of integrity. These problems are a bottleneck in the A2G network infrastructure, and the data availability will be damaged. Recently, researchers proposed designing the combination of blockchain in MEC, M2M, V2X, IoT, A2G, and UAV networks to handle security issues effectively. Therefore, blockchain in this layer and others are utilized to build a certification platform between BBU, IoT devices, and different stakeholders. Every transaction of the user is stored immutably on-chain, and the smart contracts are implemented to make dynamic user authentication to allow in the system. Generally, the A2G network's blockchain application is used to eliminate a single point failure problem and improve system trust, resource utilization, and minimize costs.

3.2. Layer-2

Virtual BBU (VBBU) pool located at a data center and various BBU nodes dynamically allocate resources to different service providers. The resources are allocated to A2G networks according to their existing demands. This layer virtualized the resources into N network slices, where BBU and Cloud are found. The Network virtualization allows network resources to be sliced and granted to multiple tenants. DRL assumes that each network infrastructure and layers decide by themselves and send information to NFV,

and the controller sends it into Cloud.

3.3. Layer-3

The main network operations, such as blockchain transaction, DRL, resource management, and computation offloading, are performed under this layer. It has three levels, network controller, UAV-BS, and Edge IoT device levels.

- Level-1:The H-CRAN with cloud computing resources is delivered by server-based applications through digital networks or through the public Internet itself. The resources which are available on the Cloud are far from edge IoT devices.
- Level-2:UAV and BS: Under this level, the UAVs are used to assist the communication in a given small cell mainly when the network is congested at a specific time, and emergency situations are existed and act as flying base station to replace the destroyed BS, and perform computational task and recharge of edge IoT devices. At this time, the edge IoT devices, mainly wireless sensors, wearable devices, and surveillance cameras, offload the collected data to UAV for further analysis and decision-making. Therefore, we consider multi-UAV enabled edge computing where UAV is considered a flying remote radio head (RRH) or base station with computation capability to assist the edge IoT device.
- Level-3: Edge IoT devices level: under this, there are ultra-dense heterogeneous devices which are connected to each other and BSs which share common resources, exchange information with the nearest devices, and have different interests. The MEC server crowed or damage when these devices request resources and need to offload their tasks simultaneously. We focus on layer three that cooperate aerial network and ground networks in blockchain-based multi-UAV-enabled edge computing for IoT scenario for QoS stability for time-sensitive tasks and low battery devices. Also, assume that there are N edge IoT devices, denoted by $U = \{u_1, u_2, ..., u_N\}$, that need to migrate computing tasks in 5G and beyond networks. Each IoT device is considered as a requester that needs computing resources from BS/UAVs. Let $E = \{e_1, e_2, ..., e_M\}$ *and* $V = \{v_1, v_2, ...v_K\}$be the set of UAVs and BSs, respectively, that serve as providers to supply computing resources and execute the computing tasks for edge IoT devices. During the computation offloading process in 5G and beyond networks, some important transmitted data may face the risk of stealing and loss, integrity violation, and data inconsistency. Thus, as shown in Figures 1 and 2, blockchain technology can easily keep track of offloading transactions' integrity and consistency when edge IoT devices transmit computing tasks to the UAVs and the BSs.

4. Conclusion

mIoT devices have been increasing over-time exponentially, and their computation capacity is very low. Thus, it needs to offload its computation task to MEC servers. This study proposed the new architecture of blockchain-based multi-UAV-enabled MEC for secure computational offloading and resource allocation in IoT networks with DRL approach in A2G network infrastructure. The UAVs are acting as an aerial base station that assists the overloaded base station and replace the destroyed base station in the cause of the natural and human-made disaster.

In future work, we will implement the proposed architecture using different schemes and blockchain and model-free DRL algorithms for secure computation offloading, and resource allocation in the multi-UAV enabled edge computing for IoT network in an emergency scenario.

References

[1] M. D. Assunc ̧Cao, R. N. Calheiros, S. Bianchi, M. A. Netto, and R. Buyya, "Big data computing and clouds: Trends and future directions," Journal of Parallel and Distributed Computing, vol. 79, pp. 3–15, 2015

[2] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "Asurvey on the edge computing for the internet of things," IEEE Access,vol. 6, pp. 6900–6919, 2018.

[3] A. M. French and J. P. Shim, "The digital revolution: Internet of things,

[4] R. Buyya and S. N. Srirama, Fog and edge computing: principles and paradigms. Wiley, 2019.

[5] N. Hossein Motlagh, T. Taleb, and O. Arouk, "Low-altitude unmanned aerial vehicles-based internet of things services: Comprehensive survey and future perspectives," IEEE Internet of Things Journal, vol. 3, no. 6, pp. 899–922, Dec 2016.

[6] S. Mohammed, S. ANOKYE, and S. Guolin, "Machine learning based unmanned aerial vehicle enabled fog-radio aerial vehicle enabled fog-radio access network and edge computing," ZTE Communications, vol. 17, no. 4, pp. 33–45, 2020.

[7] N. C. Luong, D. T. Hoang, S. Gong, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, "Applications of deep reinforcement learning in communications and networking: A survey," IEEE Communications Surveys & Tutorials, 2019.

[8] X. Xu, Y. Chen, X. Zhang, Q. Liu, X. Liu, and L. Qi, "A blockchain-based computation offloading method for edge computing in 5g networks," Software: Practice and Experience, 2019.

[9] R. A. Memon, J. Li, J. Ahmed, M. I. Nazeer, M. Ismail, and K. Ali, "Cloud-based vs. blockchain-based iot: a comparative survey and way forward." Frontiers Inf. Technol. Electron. Eng., vol. 21, no. 4, pp. 563–586, 2020.

[10] R. A. Memon, J. P. Li, M. I. Nazeer, A. N. Khan, and J. Ahmed, "Dualfog-iot: Additional fog layer for solving blockchain integration problem in internet of things," IEEE Access, vol. 7, pp. 169 073–169 093,2019.

[11] Y. He, Z. Zhang, and Y. Zhang, "A big data deep reinforcement learning approach to next generation green wireless networks," in GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE, 2017, pp.1–6.

[12] S. ANOKYE, S. Mohammed, and S. Guolin, "A survey on machine learning based proactive caching," ZTE Communications, vol. 17, no. 4, pp. 46–55, 2020.

[13] C. Zhang, Z. Liu, B. Gu, K. Yamori, and Y. Tanaka, "A deep reinforcement learning based approach for cost- and energy-aware multi-flow mobile data offloading," IEICE Transactions on Communications, p. 2017CQP0014, 2018.

[14] X. Chen, H. Zhang, C. Wu, S. Mao, Y. Ji, and M. Bennis, "Optimized computation offloading performance in virtual edge computing systems via deep reinforcement learning," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4005–4018, June 2019.

[15] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Secure computation offloading in blockchain based IoT networks with deep reinforcement learning," arXiv preprint arXiv:1908.07466, 2019.

[16] H. G. Do and W. K. Ng, "Blockchain-based system for secure data storage with private keyword search," in 2017 IEEE World Congress on Services (SERVICES), 2017, pp. 90–93.

[17] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial iot with deep reinforcement learning," IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3516–3526, 2019.

[18] O. J. A. Pinno, A. R. A. Gregio, and L. C. E. De Bona, "Controlchain: Blockchain as a central enabler for access control authorizations in the iot," in GLOBECOM 2017 - 2017 IEEE Global Communications Conference, 2017, pp. 1–6.

[19] A. Merwaday and I. Guvenc, "Uav assisted heterogeneous networks for public safety communications," in 2015 IEEE wireless communications and networking conference workshops (WCNCW). IEEE, 2015, pp. 329–334.

[20] N. Zhao, W. Lu, M. Sheng, Y. Chen, J. Tang, F. R. Yu, and K.-K. Wong, "Uav-assisted emergency networks in disasters," IEEE Wireless Communications, vol. 26, no. 1, pp. 45–51, 2019.

[21] Q. Zhang, W. Saad, M. Bennis, X. Lu, M. Debbah, and W. Zuo, "Predictive deployment of uav base stations in wireless networks: Machine learning meets contract theory," arXiv preprint arXiv:1811.01149, 2018.

[22] J. Cui, Y. Liu, and A. Nallanathan, "Multi-agent reinforcement learning based resource allocation for uav networks," arXiv preprint arXiv:1810.10408, 2018.

AN OPTIMIZATION METHOD OF JAVASCRIPT REDUNDANT CODE ELIMINATION BASED ON HYBRID ANALYSIS TECHNIQUE

GAO QIONG[1], LI WENMIN[2]

Network security center, Institute of Cyberspace Security, Beijing University of Posts and Telecommunications, Haidian district 100876, Beijing, China
E-MAIL: liwenmin02@outlook.com

Abstract:

Many websites import large JavaScript (JS) libraries to speed up development time and enhance user experience. However, many JS libraries that only partially utilized during page loading are all packaged into bundles. Redundant JS code inflates the page weight, which inflates the time it takes to download, parse, and compile JS resources. Therefore, it is very important to optimize the payload of JS resources to improve Web performance. This paper proposes a scheme combining static structure analysis technique and dynamic tracking technique to identify unused code during application execution and optimize the size of application bundle. Through the dependency relationship between the third-party libraries, this paper designed an analysis structure, which extract various types of function information to improve the redundant functions detection efficiency. After that, in the construction of the application bundle, this paper eliminated the redundant JS code. Our experiments show that the scheme is simple and effective, and reduces the amount of code in the bundle by 32.64% on average, and improves the accuracy by 23% on average compared with the coverage API redundancy detection tool. On the basis of ensuring the robustness of the code, the loading performance of the application is optimized.

Keywords:

JavaScript; Redundant function detection; Code optimization; Hybrid analysis technique

1. Introduction

Many flexible features of JS, such as no need to compile in advance, provide efficient interaction between the client and server of Web application, deepen the function of the developed website platform, and win the favor of the majority of software developers. However, such large-scale programs based on scripting language must be optimized in terms of volume. Code programs with common characteristics need to be standardized to create reusable JS libraries, such as jQuery, AngularJS, and React [1]. These libraries must be transferred to the client before each execution of the application. The size of their source code inflates the total load and prolongs the execution time of the application.

In practice, there are many ways to reduce the network transmission cost of JS. Code construction tools such as *Browserify* and *Webpack* can modularize the application and reduce the source code that is not explicitly required by the program through loading on demand. However, if the volume of the component is small, loading on demand will increase additional HTTP requests and increase the loading time. The code-splitting technology in Webpack can separate the third-party class libraries from the business code, maximize the use of browser caching mechanism and reduce requests. However, this technique do not remove unused functions from used modules. A new method called "Tree-shaking" implemented by Rollup22 tool can remove functions from modules that have not been imported through ECMA6 import/export syntax. However, this method can only detect the static structure, and can't eliminate the unused functions from the modules that have never used export syntax declarations on the basis of dynamic analysis.

This paper argues that applying JS static or dynamic analysis only is not enough to detect more precise redundant code. Dynamic analysis puts the analysis process in the actual running environment of the code. It can deal with the dynamic characteristics of JS that is difficult to achieve by analyzing the source code process [2]. Static analysis can fill the coverage problem caused by the design of test cases and input parameters, thereby making the analysis results more complete and more reliable [3].

The main contributions of this paper are as follows:

(1) On the basis of application modularization and simplification, a simplification scheme of function granularity is proposed, which refines the granularity of

detecting redundant code, and provides more possibilities for reducing the size of application bundle, improving the loading efficiency and improving the utilization of cache space.

(2) A new static analysis structure is proposed to build function call graph. By extracting information from various types of function declaration and function call, the detection accuracy of redundant functions can be improved.

(3) A hybrid analysis method integrating dynamic analysis tracking and static structure detection is proposed to improve the accuracy of detecting unused functions and simplify the identified redundant functions.

The remaining structure of this paper is as follows: Section 2 introduces the design and implementation of redundant code optimization scheme based on hybrid analysis technique. Section 3 evaluates the performance of the optimization tool to demonstrates the effectiveness of the scheme. Section 4 summarizes and outlines our future work.

2. Design and implementation of redundant code optimization scheme based on hybrid analysis

2.1. Overview

Before analyzing our target code, we need to reduce the volume of code analysis, simplify the complex association of the analyzed code, and obtain meaningful JS code set. It is necessary to divide the application source code and the third-party library code, and then group them according to the corresponding relationship between HTML pages and JS resources to match the optimization idea of page loading on demand. For JS resources shared by multiple groups, we uniformly detect them to avoid repeated calculation.

Figure 1 shows the process of redundant code optimization scheme: it is mainly divided into two phases, the first phase is learning phase, including static analysis and dynamic analysis. In the static analysis process, the JS code to be analyzed is first parsed into an abstract syntax tree (AST), and then the function information is extracted by traversing the AST. A function call graph is built according to the above extracted function information and function call relationship to identify redundant functions. After that, the refactored code is dynamically executed to collect execution information. The second phase is the reduction phase. Combined with the data collected in the first phase, the unused functions in the application dependency library are identified and eliminated. Finally, the optimized JS code is output to provide developers with the next step of deployment.

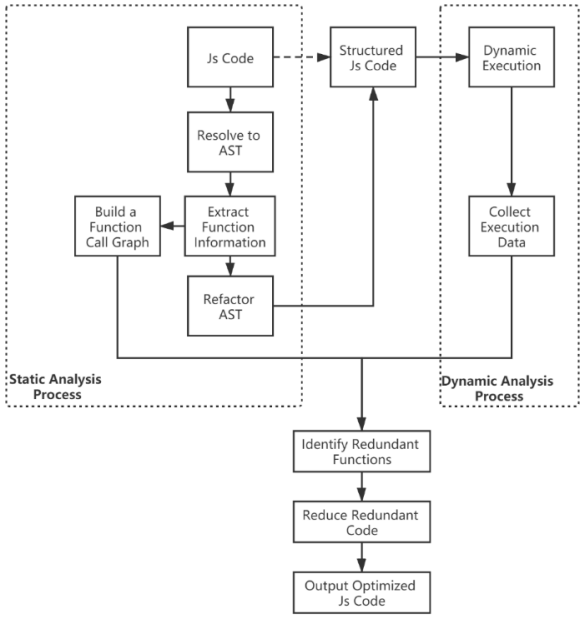


Fig.1 Overview of our approach

2.2. Module processing

Since the optimization scheme in this paper is mainly aimed at the unused function code in the required module of the application, we need to modularize and simplify the application code before identifying the unused code. We use the packaging tool $Browserify$ to traverse the dependencies between modules and discard those that are not needed. $Browserify$ allows user to organize JS code on the browser side in a way similar to $require()$ in Node.js. In fact, it provides the function of NPM module manager for browser indirectly. When a module uses $require$ to load a third-party library or other modules, its dependent modules and dependent third-party libraries will be bundled together to bundle.

2.3. Static analysis

To analyze JS code, you must convert it into a form that the tool can recognize according to its rules. This paper first parses each JS file into an AST through esprima.js, and adds file name information to the root node of the tree. Then, multiple ASTs are merged into one AST for analysis.

When the existing Chrome coverage detection tool Coverage API performs static analysis on JS resources, it can only capture general function calls, but ignores the use of anonymous functions in JS resources, and reports all

anonymous functions as redundant [4]. The static analysis method designed in this paper considers a variety of ways of function declaration modes and function call modes, and constructs different information extraction structure according to different declarations and calling modes to extract information related to parameters and parameter types respectively.

Function declaration information: As show in the following 7 tuples (1). $file$ identifies the file name where the function is located, $name$ indicates the function name, $anonymous\_id$ represents the anonymous function id, which is an auto increment id, and it is assigned only when the function name is null, otherwise it is null. $start\_line$ is the line number where the function starts, end_line is the line number where the function ends, $comment$ represents the function comment, that is, the comment information written in front of the function declaration, and $params$ is the parameters of the function, which is in the form of array.

$$< file, name, anonymous_{id}, start_{line}, end_{line}, comment, params > \quad (1)$$

Function call information: The information of the function call to be extracted is shown in the following 5 tuples (2). $line$ is the line number where the function is called, and $args$ is the parameters of the function, which is in the form of array.

$$< file, name, anonymous_{id}, line, args > \quad (2)$$

The above two parts describe the function information to be extracted. The information extraction is completed by traversing the AST. The specific information extraction process is shown in algorithm 1: JS function declaration includes five categories. The above information is extracted for each category. Lines 9-10 indicate the information collection process of function declaration. Lines 11-13 show the information collection process of the function call.

Alg.1 Function information extraction algorithm

Input: projFiles (JS files in project)
Output: defInfo, callInfo (All information about function declaration and function call in a project)

```
1  Begin
2    defInfo ← []
3    callInfo ← []
4    For Each file ∈ projFiles do
5      script ← fs.readFileSync(filePath, 'utf-8')
6      ast ← esprima.parseScript(script)
7      estraverse.traverse(ast, {
8      enter: function(node) {
9        If node.type == 'FunctionDeclaration'
10             || node.type == 'VariableDeclaration'
11             || node.type == 'ClassDeclaration'
12             || node.type == 'ObjectExpression':
13         info ← extractDefInfo(node)
14         defInfo ← defInfo ∪ {info}
15       Elif 'CallExpression':
16         info ← extractCallInfo(node)
17         callInfo ← callInfo ∪ {info}
18       End If
19       }
20     }
21   End For
22 End
```

After extracting information, the function declaration and function call can be linked by function name or id to obtain a definition-call pair, and finally a JS function call graph with relevant functions and parameter information is obtained. The functions that do not appear in the function call graph, that is, there is no definition call pair, are identified as redundant functions.

2.4. Dynamic execution tracking

In order to track the application code dynamically, we need to do the instrumentation in advance. In the process of traversing AST, once the function is identified, an instruction is added at the beginning of the function. This command records execution information to a file during the running time, so that it records whether the function was executed.

For example, application $messy$ (object model of HTTP message) relies on the library $underscore$ and library $encoding$. Once we call the function $toJSON$ in $messy$, it will trigger a series of calls involving library functions through the dependency chain, such as the function $createAssigner$ in the $underscore$, function $toUTF8$ and function $encode$ in the $encoding$ [5]. Then, the dynamic execution tracing will generate information fragment as shown in Table 1:

Table 1 Execution information fragment

1	function $createAssigner()$ defined in /underscore/ underscore.js was executed.
2	function $toUTF8()$ defined in /underscore/ underscore.js was executed.
3	function $encode()$ defined in /encoding/ encoding.js was executed.

2.5. Redundant code elimination

Removing unused code is challenging, partially due to the dynamic nature of JS language, such as $eval$ function, event binding, multi-type parameter transfers etc. It is possible to misjudge and eliminated due to the incomplete

test cases [6]. These dynamically referenced functions cannot be separated from the unused functions. Once we eliminate all the unused function codes, the program is likely to crash in the next execution, affecting the code stability and page health.

So our approach takes a less radical strategy. Specifically, for the redundant functions identified by detection, we retain the unique identifier and formal parameters of the function, and simplify the content of the function body, and backup the code segment to a local folder. When user operations other than test case execute these functions, a synchronous XMLHttpRequest (XHR) request is issued to download the eliminated function body, and then the JS Eval method is run on to download the function body. Appropriate context and function parameters are provided for the method to prevent the program from reporting errors or inaction.

3. Experiment and analysis

In order to evaluate the method of optimizing redundant functions in this paper, the author implements a detection tool based on Nodejs. The tool takes the whole JS project as input. It can automatically ignore the redundant modules in the project, eliminate the redundant functions in the required module, and perform dynamic tracking to improve the execution information, so as to avoid misjudgment. In terms of experimental objects, we considered 15 popular open source JS projects on GitHub. The specific information of the project is shown in Table 2.

Table 2 Experimental data set

JS Application	Bundle LOC	#Functions in bundle	Minified bundled size(bytes)
Chart.js	13728	1044	187074
angularjs-countdown	24,094	1219	136697
Backbone-tableview	11350	978	136054
chomsky	20029	2064	242023
escodegen	4946	370	99161
escope	7565	604	97853
geojsonhint	2022	109	30801
mathjs	50885	2865	507702
messy	22405	504	441294
mochawesome	11255	936	154656
transform-pouch	1467	214	27899
underscore.string	1600	170	31935
unexpected-http	39037	1923	584046
unexpected-messy	36942	1766	557454
workfront-api	16207	930	226744
Mean	17569	1046.4	230759.53

In order to better evaluate the effectiveness of this scheme, we propose the following research questions.

RQ1: How many redundant functions can be detected by the scheme proposed in this paper, and how much is the code size reduced after optimization?

RQ2: How does the scheme in this paper compared with the Coverage API detection tool to detect redundant functions?

RQ3: How does the hybrid analysis technique based on integrated dynamic analysis tracking and static structure detection compared with the static analysis technique only and the dynamic analysis technique only?

For RQ1, when running the optimization tool implemented in this paper, we found that there are 6378 redundant functions in the bundle, which means that 40.63% of the functions in the bundle are unused function. In addition, these redundant functions contain a large number of lines of code, accounting for 27.95% of the code in the original bundle.

Table 3 Experiment results

JS Application	#Redund-ant functions	LOC of elimina-tion	Improved bundle size	% of reduc-tion
Chart.js	289	1558	160916	13.98%
angularjs-countdown	856	6852	57680	57.80%
Backbone-tableview	632	4838	68551	49.61%
chomsky	1054	5572	149236	38.34%
escodegen	107	1057	81392	17.92%
escope	201	2091	70352	28.10%
geojsonhint	14	88	28628	7.05%
mathjs	72	631	500731	1.37%
messy	361	12509	149289	66.17%
mochawesome	631	5109	73690	52.35%
transform-pouch	78	326	20454	26.69%
underscore.string	8	36	31277	2.06%
unexpected-http	993	15613	232836	60.13%
unexpected-messy	833	16043	215361	61.37%
workfront-api	249	1346	211619	6.67%
Mean	425.2	4911.3	136801	32.64%

Table 3 shows the experimental results of redundant

function detection and optimization. Compared with the original bundle size, the optimized bundle size is reduced by 32.64% on average. It can be seen that the elimination tool implemented in this paper can effectively identify the redundant functions of the required module, and can significantly reduce the bundle size, and improve the loading efficiency while ensuring the robustness of the code.

For RQ2, we run 15 JS projects on the Chrome browser to obtain the execution information and compare it with our method. In order to clearly consider the accuracy of the detection tools, we use the precision and recall indicators in the information retrieval field to analyze [7]. In this section of the experiment, when analyzing the JS application w , the accuracy P_a of the analysis technique a is defined as:

$$P_a = \frac{|D_a(w) \cap D_t(w)|}{|D_a(w)|} \quad (3)$$

Where $D_a(w)$ is the set of functions identified as redundant by the analysis technique a and $D_t(w)$is the set of true redundant functions in w. Intuitively, precision deals with false positives, it can be seen as the fraction of JS functions identified as redundant by analysis a that are true redundant functions [4].

The recall R_a of analysis technique a when analyzing JS application w is defined as:

$$R_a = \frac{|D_a(w) \cap D_t(w)|}{|D_t(w)|} \quad (4)$$

Recall deals with false negatives, and it is defined as the fraction of JS functions identified as redundant by the current analysis, over the total amount of true redundant functions contained in the application.

Figures 2 and 3 show the precision and recall results of our method and Coverage API respectively. It can be seen that our method is better than Coverage API in terms of precision and recall rate. This is because that the Coverage API cannot capture the usage of anonymous function declarations and reports all anonymous functions as redundant. In our other research experiments, the proportion of anonymous functions in JS resources is a very large part. The second reason is that the JS resources in the application source code and the third-party library are not separated in the detection process of Coverage API, resulting false alarms [4].

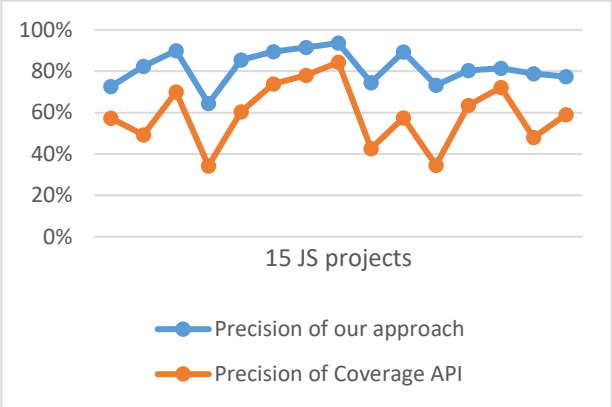


Fig.2 Precision of two approach

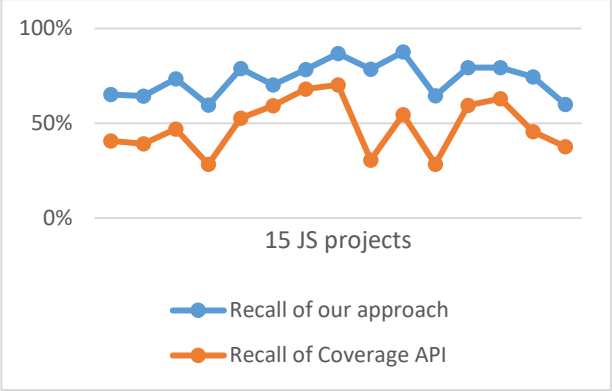


Fig.3 Recall of two approach

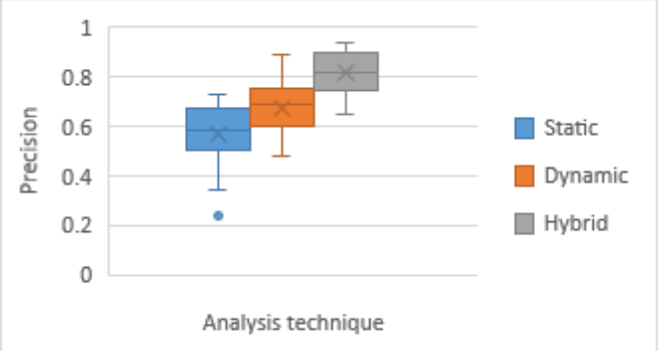


Fig.4 Precision of three analysis technique

For RQ3, we compare the precision and recall of static analysis technique only, dynamic analysis technique only, and hybrid ones. Figure 4 shows the distribution of precision. The experimental results show that compared with static analysis technique only (average=0.56, median=0.58) and dynamic ones (average=0.67, median=0.69), hybrid analysis technique (average=0.82, median=0.82) preformed more accurate. This is because that static analysis and dynamic analysis obtain the execution status in different ways. During

the merging phase, the number of redundant functions identified will be reduced to the greatest extent. Therefore, the precision of the hybrid analysis technique is high and stable. After merging phase, those still identified as redundant functions have a greater probability of being the true redundant results.

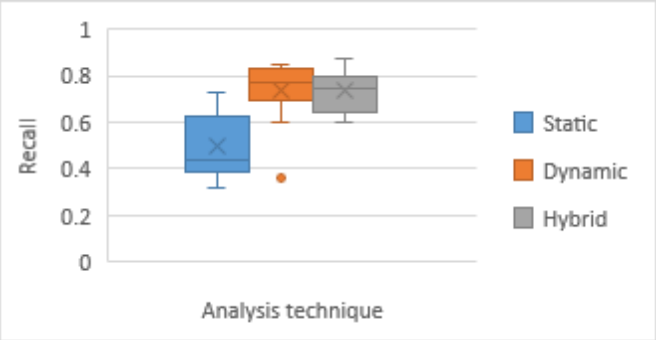


Fig.5 Recall of three analysis technique

Figure 5 shows the distribution of recall. It can be noticed that the recall of dynamic analysis technique only (average= 0.73, median=0.77) and hybrid ones (average=0.73, median=0.75) are better than static analysis techniques only (average=0.49, median =0.44). This is due to two main reasons. First, many JS applications in dataset import third-party libraries that usually contain a large number of JS functions, but they only use a small part of these libraries; Dynamic analysis can correctly identify unused functions as redundant. Second, the business logic of the considered application is quite minimal; This is reflected in a low number of application-specific JS functions which may not be executed during dynamic analysis [8].

In general, the experiment show that the new static analysis structure and the combination of analysis technique improve the precision of detecting redundant functions and reduce the false alarm rate. However, from the perspective of recall rate, the hybrid analysis technique does not improve much compared with dynamic analysis technique only. This may be due to the inaccurate merging rules in the process of merging, and the dynamic tracking process does not consider the situation that real users clicking to load JS resources. so in future work, more expansion of merge rules will be added, and real user operations will be monitored to improve the accuracy of redundant functions.

4. Conclusions

For a more beautiful page design and functional interaction experience, website developers usually introduce packaged third-party libraries to save development costs. However, these libraries are usually only partially used, all of them are packaged into the bundle, resulting in a large amount of redundant code on the website that must be downloaded, decompressed and parsed before execution. In this paper, we use static structure analysis combined with dynamic execution technique to identify and eliminate redundant JS code. The evaluation results show that the scheme can effectively reduce the amount of redundant code in application bundle, reduce page delay time, and improve code download and execution efficiency. The research purpose of this paper is not only to guide developers to detect and simplify JS resources, but also to stimulate the demand for website performance optimization. Whether it is adaptation requirements for different devices or diverse ecological environments, the ultimate goal is to improve the user experience.

References

[1] Farzat F , Barros M O , Travassos G H . Evolving JavaScript code to reduce load time[J]. IEEE Transactions on Software Engineering, 2019, PP(99):1-1.

[2] S.H. Jensen, A. Møller, P. Thiemann, Interprocedural analysis with lazy propagation, in:Proceedings of the International Static Analysis Symposium, Springer (2010), pp. 320-339.

[3] S. Benschop, Efficient Approximate JavaScript Call Graph Construction, University of Groningen. (2014) Master's thesis

[4] Goel U , Steiner M . System to Identify and Elide Superfluous JavaScript Code for Faster Webpage Loads[J]. 2020.

[5] Vazquez H C , Bergel A , Vidal S , et al. Slimming javascript applications: An approach for removing unused functions from javascript libraries[J]. Information and software technology, 2019, 107(MAR.):18-29.

[6] Tan T H , Xue Y , Chen M , et al. JSFox: Integrating Static and Dynamic Type Analysis of JavaScript Programs[C]// International Conference on Software Engineering Companion. ACM, 2017.

[7] Obbink N G , Malavolta I , Luca G , et al. An extensible approach for taming the challenges of JavaScript dead code elimination[C]// International conference on Software Analysis, Evolution and Reengineering (SANER). IEEE Computer Society, 2018.

[8] Jiho Choi, Reusable Inline Caching for Javascript Performance, PLDI 2019（40th ACM SIGPLAN Symposium on Programming Language Design & Implementation）889-901.

CONSTRUCTING NAIVE BAYESIAN CLASSIFICATION MODEL BY SPARK FOR BIG DATA

WANG XIAOFANG[1], LUO LAN[1], ZOU QIANYIN[1], LIU FENGYU[1], LIU JIAWEI[1], HUANG DI[1]

[1]Chengdu College of University of Electronic Science and Technology of China, Chengdu, 611731, China
E-MAIL: luolan@cduestc.edu.cn

Abstract:

Due to the development of big data technology, traditional machine learning algorithms are difficult to deal with massive data. To solve this problem, a naive Bayesian classifier based on parallel training and prediction on Spark platform is proposed. The classifier includes Laplace smoothing and normal distribution functions. Bayesian classification algorithm combined with Spark distributed platform to build a complete functional naive Bayesian model for data mining and data analysis and testing. Experimental results show that the accuracy of MLlib -based optimized continuous feature vector dataset is 9.75% higher than that of the traditional naive Bayes classification algorithm.

Keywords:

Spark; Classifier; Naive Bayes; Data Mining

1. Introduction

Big data technology in recent years is ushering in a critical period of development, when a large number of data how to collect, how to store, how to calculate the problem. How to efficiently use data mining technology to mine data value is the current research topic[1-5]. This paper presents an optimization algorithm for Spark's MLlib naive Bayesian classification. This algorithm is a naive Bayesian algorithm based on normal distribution model. The data distribution will use normal distribution function to classify the data and get the feature vectors, so as to optimize the continuous feature vectors[5-8].

The Spark MLlib (Machine Learning Library) is a library of commonly used machine learning algorithms based on Spark, including related test and data generators[9-11]. Spark MLlib aims to simplify the engineering practices of machine learning for easy scalability to larger scale, common learning algorithms and tool components, including classification, regression, clustering, collaborative filtering, dimensionality reduction, etc., currently supports four machine learning problems: classification, regression, clustering and collaborative filtering[12-13].

2. Relevant Work

2.1. A Naïve Bayesian Algorithm

Naive Bayes classification algorithm [14] is a kind of classification algorithm based on Bayes theorem. It assumes that all the samples are independent events, and the amount of independent calculation of the samples is greatly reduced.

$$p(y_i|x) = \frac{p(x|y_i)p(y_i)}{p(x)} \quad (1)$$

Among them, the denominator for all categories are constant, and each characteristic attribute is independent, from the formula (1) to further derive conditional probability formula, as shown in formula 2.

$$p(y_i|x)p(y_i) = p(a_1|y_i)p(a_2|y_i)\cdots p(a_m|y_i) = p(y_i)\prod_{j=1}^{m} p(a_j|y_i) \quad (2)$$

In Naive Bayesian Algorithm, $p(y_i)$ of each class needs to be calculated in the model training stage, and conditional probabilities of all partitions are calculated for each feature attribute. In the stage of model prediction application, we need to calculate the $p(y_i|x)p(y_i)$ of each category based on the existing probability, and find out the largest term as the category of x.

2.2. Binary function immunity

If any of the m arguments in $f(x)$ are statistically independent of $x_1, x_2, \ldots x_n$,then f is said to be m order dependent, and its first order immune function [15] is shown in Formula 3.

$$F(x_1, x_2, x_3, x_4) = x_1x_2 + x_3 + x_4 \quad (3)$$

The truth table for first-order immune functions is

shown in Figure 1.

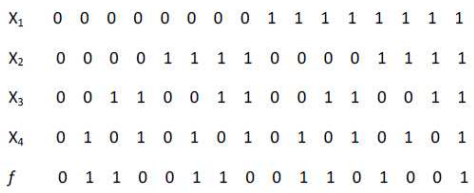


Fig.1 First-order function value-added graph

As can be seen from Fig. 1, the true value of the original function f is 8 zeros and 1, respectively, and the equilibrium function is shown in Form 4.

$$|\{f(x)=0 \mid x \in F_2^n\}| = |\{f(x)=1 \mid x \in F_2^n\}| = 8 \quad (4)$$

For the first order immune function, when $X_i = 0$ or $X_i = 1$, the number of true values of f function is 4 respectively, and its equilibrium is the first order immune correlation function.

$$\begin{cases} |\{f(x)=0 \mid x_i=0 \in F_2^n\}| = 4 = 8/2 \\ |\{f(x)=0 \mid x_i=1 \in F_2^n\}| = 4 = 8/2 \\ |\{f(x)=1 \mid x_i=0 \in F_2^n\}| = 4 = 8/2 \\ |\{f(x)=1 \mid x_i=1 \in F_2^n\}| = 4 = 8/2 \end{cases} \quad (5)$$

But for the second order, when we take $x_3 = 0$, $x_4 = 0$, the number of functions with f being 0 is 3, and the number of functions with 1 is 1, which is unbalanced. The formula is shown in formula 6.

$$\begin{cases} |\{f(x)=1 \mid x_3=x_4=0 \in F_2^n\}| = 1 < 8/2 \\ |\{f(x)=1 \mid x_3=x_4=0 \in F_2^n\}| = 3 > 8/2 \end{cases} \quad (6)$$

From the above expression, we know that the non-second order function is correlation immunity.

3. Algorithm implementation.

3.1. Environmental deployment

Table 1 Experimental Environment

development environment deployment		
Apache Spark	2.3.0	computing platform
Java	1.8.0_161	implementation language
Scala	2.11.12	concurrent container
Ubuntu	16.04	development environment
Kaggle	umakantjena2015	contrast test data source

As can be seen from Table 1, the vector calculation part of this experiment uses Apache Spark dependent breeze mathematical calculation library, implemented in Scala language, installed Scala version 2.11.12 software.

In the implementation of Spark's official MLlib Naive Bayes algorithm, although MLlib Naive Bayes algorithm realizes polynomial model and Bernoulli model, it is not good at predicting continuous feature vectors because MLlib has other classification algorithms that can be used for continuous feature vectors. In this paper, we introduce the Naive Bayes algorithm based on binary immune. In this algorithm, the data distribution is realized by normal distribution function, which can optimize the continuous eigenvectors in the Naive Bayes model.

3.2. Algorithmic implementation

The implementation of the algorithm is divided into four parts: breeze compatibility layer, encapsulated model and feature object implementation, algorithm core implementation and normal distribution function implementation.

3.2.1. Probability caculation

Because of the lack of training data, the quality of the classifier may be degraded greatly when the calculated feature attribute is 0 for a certain class. In this paper, Laplace smoothing calibration is used for smoothing, and lambda parameter is introduced as smoothing factor for corresponding calculation.

$$p_\gamma(x_{ij}|y_k) = \frac{\sum_{i=1}^{N} p(x_{ij},y_k)+\gamma}{\sum_{i=1}^{N} p(y_k)+S_j\gamma} \quad (7)$$

$$p_\gamma(y_k) = \frac{\sum_{i=1}^{N} p(y_k)+\gamma}{N+K\gamma} \quad (8)$$

Of these, x_{ij} represents the i category of the j feature, S_j represents the number of the j feature, and K represents the number of categories. Set γ to 1 to avoid the probability of 0, and ensure that each probability value is between 0 and 1. Solve the problem of computing characteristic attribute to a class probability of 0.

After smoothing, the characteristic probability calculated by Naive Bayes Algorithm can be either continuous or discrete, and the discrete value can be used to calculate the probability of each class in the training sample directly, but the continuous characteristic attribute is not available. In order to solve this kind of problem, we set the continuous value to obey the normal distribution and adopt the normal distribution method. In this algorithm, the normal distribution is used to process the data and train it, which ensures that the probabilistic information is transformed into the mean and variance of the model, and the data is processed more efficiently and quickly.

3.2.2. Spark platform running

Before running, it is necessary to set up the corresponding project and write the concrete code. The code is written in Java language, and the concrete engineering structure is shown

3.2.3. Functional implementation

DenseVectorSupport.scala is a Scala Object class for all static methods in Java that contains seven methods covering vector addition, subtraction, multiplication, and division creation and two specific vector operations for algorithmic implementation.

The reason for adding a serialized interface is that any object computed in Spark requires a serialized transport. If you don' t serializes it, the run will throw an exception, so you need to add the interface implementation, which is also well suited to Java lambda expressions.

LabeledPoint is a typical class of Java bean objects where the data is immutable, so there is no set method provided, and its members are decorated with the final keyword. This class completely describes the class to which a piece of data belongs and its corresponding characteristics, where the feature vectors are described using the breeze library's DenseVector.

Because of the partial incompatibility of generic types, the Java code called the compatibility layer function to remove the generic constraints, but consider the upper level of input data processing implementation, to ensure type safety.

In the implementation of a Bayesian model object, the model preserves the training effort and has a way to serialize the model file to disk for direct use next time

4. Experimental result

A naive Bayesian classification model data set from the Kaggle platform was used in this comparative test. The information in the data set was five different wines, and the number of wines in each wine variety. Each wine contained six different characteristic parameters, such as alcohol concentration, mellow or soy flavor, which described the specific types of wines.

In contrast testing, the data sets are randomly divided into one-third of the data sets, excluding the data of these test data sets as training sets.

The comparison test uses the Naive Bayes algorithm implemented by RDD API and the Naive Bayes algorithm implemented by Spark based on the normal distribution of Spark.

The contrastive test uses exactly the same logic and parameters, uses the same training set data, predicts the same testing set data, and compares it with the correct answer to get the final accuracy. Run the program as shown in Figure 2.

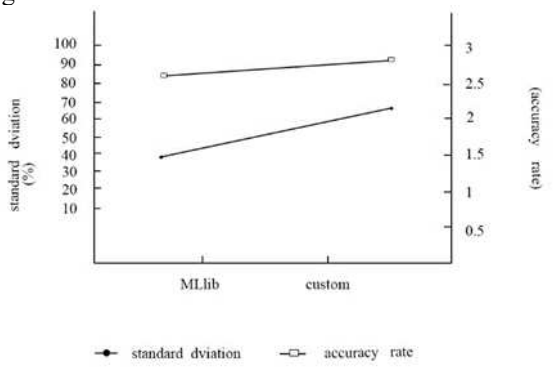


Fig.2 MLlib model contrast test results

As can be seen from figure 2, the prediction accuracy of Spark MLlib's naive Bayes model is about 82.93%, the standard deviation is 2.3, and the realization accuracy of the custom model is about 92.68%, the standard deviation is 1.5, the accuracy of the custom model is 9.75% higher than that of Spark MLlib's naive Bayes model, and the variance is smaller.

5. Conclusions

In this paper, we propose to apply Conditional Bayesian Algorithm based on binary immune processing to Spark, which is faster and more accurate than traditional conditional Bayesian Algorithm. In this model, the small-scale data simulation of large data screening is used to verify that the model is suitable for intelligent recommendation of e-commerce, related data mining and other scenarios. Through the binary immune processing of model reference, the time spent on the model is higher than that on the Spark platform.

References

[1] Lan Luo, Fengli Zhang, ShiJie Zhou.A Design Of Data Security Algorithm To Trusted Network Connect and comment to Its Security[C], Proceedings of 2006 Symposium on Information. ChengDu:Electronics and Control Technologies, 2006:28-36.

[2] Weiya Chen,Chun Yao,Yingzhong Guo,etc. pmTM-align: scalable pairwise and multiple structure alignment with Apache Spark and OpenMP[J]. BMC Bioinformatics,2020,21(1).

[3] Niraj Chawake,Lavanya Raman,Parthiban Ramasamy,etc,Christoph Gammer,B.S. Murty,Ravi Sankar Kottada,Jürgen Eckert. Composite of medium entropy alloys synthesized using spark plasma sintering[J]. Scripta Materialia,2021,191.
[4] Zhong Xiao, Ma Shaoping, etc. Data Mining Overview [J]. Pattern Recognition and Artificial Intelligence, January 14, 2001 (1): 48 ~ 55.
[5] Wang Zhenyu, Guo Li. Analysis of Hadoop -based Search Engine User Behavior [J]. Computer Engineering and S,2016:4.
[6] Hisao BANNO. Dielectric and Electromecanical Properties of Soft PZT-family Ceramics Containing WO_3 Component and Their Applications to Electromecanical Transducers[A].IEEE Components,Hybrids and Manufacturing Technology Society,1989:2.
[7] Weiya Chen,Chun Yao,Yingzhong Guo,etc. pmTM-align: scalable pairwise and multiple structure alignment with Apache Spark and OpenMP[J]. BMC Bioinformatics,2020,21(1).
[8] Taizhi Lv,Juan Zhang,Yingying Chen. Job Analysis System Based on Spark Platform[A]. Institute of Management Science and Industrial Engineering.Proceedings of 2020 3rd International Conference on Financial Management, Education and Social Science(FMESS 2020)[C].Institute of Management Science and Industrial Engineering: Computer Science and Electronic Technology International Society,2020:5.
[9] Jacques G. Noudem, Yiteng Xing, Pierre Bernstein, etc. Masato Murakami. Improvement of critical current density of MgB2 bulk superconductor processed by Spark Plasma Sintering[J]. Journal of the American Ceramic Society,2020,103(11).
[10] Anna Karen GARATEESCAMILLA, Amir HAJJAM EL HASSANI, Emmanuel ANDRES. Big data scalability based on Spark Machine Learning Libraries[A].SCIence and Engineering Institute(SCIEI),2019:6.
[11] Aoxiang Peng,Huiyong Liu. Hybrid Program Recommendation Algorithm Based on Spark MLlib in Big Data Environment[C]. Proceedings of the 9th International Conference on Computer Engineering and Networks(CENet2019),2019:9.
[12] Lei Cao, Jingfeng Hu, Ran Li. Construction and Application of Ship Data Mining Platform Based on Spark[C]. Science and Engineering Research Center. Proceedings of 2019 International Conference on Modeling. Science and Engineering Research Center, 2019:6.
[13] Yuyang Wang, Tianlei Zhou. A Lowest Cost RDD Caching Strategy for Spark[C]. Institute of Management Science and Industrial Engineering. Proceedings of 2019 4th International Conference on Automatic Control and Mechatronic Engineering (ACME 2019), 2019:7.
[14] Huan Zhang, Liangxiao Jiang, Liangjun Yu. Attribute and instance weighted naive Bayes[J]. Pattern Recognition,2021,111.
[15] Zhu JD, Zhong Y. Feature selection method based on parallel binary immune quantum particle swarm optimization [J]. Control and decision, 2010, 25 (01): 53-58.

IMPLANTING BIG DATA TECHNOLOGY INTO THE CONSTRUCTION OF "SMART PARKING"

CHENG YANG[1], XIONG. SHIYONG[2]

[1] Software Engineering Department, Faculty of Software Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400000, China
[2] Data Media Technology Institute, Chongqing University of Posts and Telecommunications, Chongqing 400000, China
E-MAIL: 272474383@qq.com, 465898137@qq.com

Abstract:

As my country attaches more and more importance to the construction of smart cities, the construction of smart parking is gradually becoming more mature. With the advent of the big data era, data analysis is becoming more and more important in the construction of smart parking. Big data analysis can not only effectively use idle data, but also provide government managers with effective, accurate, and real-time data support, thereby improving the efficiency of managers' planning and management of parking lots. This paper mainly studies the current complex parking situation in Tongliang District of Chongqing City, and uses big data technology to replace traditional data management methods to solve the current problems of parking business in Tongliang District, Chongqing City.

Keywords:

Tracking; Smart parking; Big Data; Data management

1. Introduction

So far, the development of smart parking has become more and more mature in my country, which is mainly reflected in the increasing maturity of corresponding parking software and parking lot planning and management. At present, there are a large number of smart parking software on the market that help drivers to park efficiently. These software reduce the problem of user parking difficulties from the user side. As a large number of intelligent hardware equipment is put into use in the parking lot, the utilization efficiency of the parking lot is greatly improved, and the labor cost of the parking lot is also reduced.

With the intelligentization and diversification of intelligent parking software and parking lot management equipment and software, a large amount of parking data cannot be managed uniformly and effectively, and the value of the data itself has not been reflected.

Starting from 2019, Tongliang District of Chongqing will centralize the management of parking lots in the whole Tongliang district, collecting and managing the data of more than 8,700 parking Spaces (road parking and parking lots) in more than 380 parking lots in the district. Build a big data platform for centralized management and analysis of collected data, and provide effective, accurate and real-time data support for government management departments, so as to improve managers' planning and management efficiency of parking lots and reduce unnecessary labor costs (field trips).

This paper mainly studies the big data platform construction design and big data analysis model design in Tongliang District.

2. Smart parking big data platform design

According to the current operation of the parking lot in Tongliang District, Chongqing, as shown in Fig.1, this article will design the intelligent parking lot big data analysis platform from the following four levels: base layer, data layer, system layer and application layer.[1]

2.1. Base layer

In the base layer, HPC hardware is the base of building stable and extensible architecture. Integrate existing servers and storage, use cloud technology systems such as Citrix and VMware, and adopt virtualization technology to support cloud storage and cloud computing services, so as to form a data resource pool for unified data management. The basic resource pool can be divided into two types: small area (3-5 parking lots) and large area (3-5 small areas). The classification of resource pools can not only meet the cloud computing capacity of intelligent parking platform required by big data environment, but also make data management more convenient.

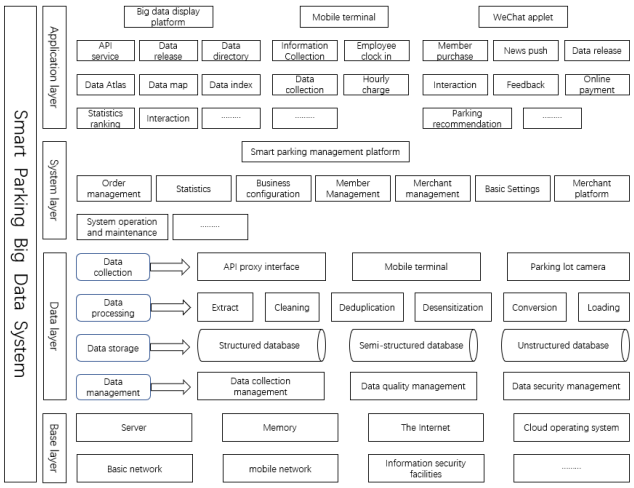


Fig.1 Big data framework

2.2. Data layer

The data layer mainly analyzes the business data, constructs the corresponding data storage structure and carries on the efficient storage and management to the collected data. As shown in Fig.2, it is mainly completed by the following steps: data acquisition, data processing, data storage and data management.

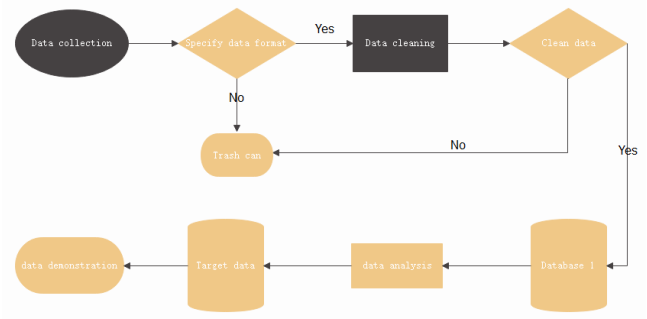


Fig.2 Data flow chart

Data collection

At present, the data collection methods of parking lot in Tongliang District of Chongqing are mainly divided into two ways: scanning code collection by gate machine and mobile terminal machine. Due to the differences in data acquisition equipment and background management system adopted by many parking lots, there will be differences in data types when the big data platform collects data from these different car yards. In the process of data collection, it is necessary to unify the data collection format according to the data requirements of government agencies.

Data processing

Data processing adopts offline batch processing and real-time processing in parallel.

Offline batch maxComputer is a fast and fully managed TERabyte/petabyte data warehouse solution. According to the requirements of government agencies, we set the execution time and conditions of tasks, and the corresponding data we need every day will be obtained.

Real-time processing: Task execution conditions are set as for offline batch processing as required by government agencies, but the execution time is real-time. The collected data are processed and analyzed in real time to ensure the real-time performance of the data. Compare the obtained data with the offline batch data to ensure the validity and accuracy of the data. In both cases, non-relational database is used for data storage.

Data storage

In data storage, there are two stored procedures of data. The first storage occurs when the data is collected in a unified format. The second storage occurs when the data is obtained after processing the first storage. In this study, we chose MongoDB to store the data. Currently, the mainstream non-relational databases include MongoDB and HBase. MongoDB is more efficient than HBase in both import and export of data, so MongoDB is selected in the study.

Data management

Data management is mainly through the construction of the corresponding data management platform for data management. The data to be managed is not only the parking data collected by the parking lot, but also the user data bound to the vehicle, the fee administrator data, the performance of the parking lot fee, etc. This is detailed in Section 1.3.

2.3. System layer

The system layer is composed of a smart parking system management platform, which includes modules such as parking lot management, personnel management, authority management, and account management.

Parking lot management: Parking lot management includes the setting and management of basic parking lot information such as the number of parking spaces, business hours, billing rules, parking lot associations, and monthly ticket management.

Personnel management: Personnel management mainly refers to the setting and management of on-street parking administrator information, related parking lots, and attendance.

Authority management: Authority management mainly sets the authority and function of the system platform

account, and sets it according to the responsibilities performed by the account user.

Account management: Account management mainly includes operations such as registering employee accounts, setting information, and changing passwords.

2.4. Application layer

The application layer mainly includes Big data platform, WeChat small programs, and mobile terminal APP. The big data platform is mainly a data support platform for government management agencies to inquire data and observe data fluctuations and trends of parking lots, it provides the management organization with the most intuitive data from the big data platform and data analysis, So that the manager according to the data feedback reasonable to the car yard management adjustment and related rectification. WeChat small program mainly provides drivers with the functions of optimal parking recommendation, parking payment, historical record inquiry, member handling and so on. The mobile APP is mainly provided to some parking lot fee payers, its main functions include vehicle registration, charging fees and punching in time, it is also an important way to collect parking data. [2]

3. Data analysis model design

Through big data analysis technology, the collected parking data is analyzed in real time. In the whole process of analysis, the study of model selection and design is the most critical step. The research of analysis model includes two parts: element analysis and model research.

3.1. Factor analysis

In this study, the big data analysis of vehicle yard data is mainly to provide data support and solutions for the supervision work of government departments and the planning of vehicle yard. The analysis elements involved in data analysis should be based on the business scenarios and requirements of government departments.[3] It includes the following important analysis elements:

Parking capacity: Parking capacity refers to the specific number of parking Spaces.

Number of parking: The total number of daily, monthly and quarterly parking Spaces in each parking area. The number of parking Spaces is an objective factor to judge the flow of people and vehicles around a parking lot.

Utilization rate of parking space: Utilization rate of parking space refers to a mean value of the parking space occupancy rate in a certain period of time. It is also an important factor to measure the utilization efficiency of parking spaces.

Parking rate of change: Parking rate of change refers to the difference between the two periods of parking space utilization in the same parking lot, and is an indicator that describes the fluctuation of parking space utilization in the same parking lot.

Parking flow: The parking flow refers to the situation of moving vehicles in and out of a period of time.

Daily turnover: the total daily profit of a single parking lot from 8:00-21:00.

Daily arrears: the amount of profit that a single parking lot has not received in a single day from 8:00-21:00 (total arrears = total receivables-total profit).

Parking lot comment area: parking users can make star ratings and comments on the selected parking lot through the WeChat applet.

3.2. Model study

Model design

Preliminary design of data analysis model according to analysis elements and government demand. Select the appropriate type of analysis model and carry out data analysis experiment on the designed analysis model. The data analysis model with the best accuracy, the highest efficiency, the smallest error and the most suitable can be obtained through the constant modification and experiment of the model.

Analysis method design

According to the analysis model, select the appropriate big data analysis method to analyze the data in the analysis model. The analysis methods selected in the research process include the following:

Cluster analysis: Bundle the related data in the parking lot data in the big data platform, and then analyze the data through the analysis model.

Predictive analysis: Carry out predictive analysis on historical data collected in the big data platform to predict a change in future data.

Correlation analysis: The correlation analysis of the data results obtained from the forecast analysis is carried out to infer the response of the government agencies to the car yard management and car yard planning required by the analysis results, and the scheme is recommended to the government departments. [4]

3.3. Analysis model improvement

In order to improve the analysis efficiency, reduce the

error and improve the accuracy in the data analysis process, it is necessary to carry out continuous experiments on the analysis model and methods and compare the experimental results. As shown in Figure 3, the optimal data analysis model is obtained through repeated training, evaluation, application and optimization of the analysis model. Similarly, it is also necessary to continuously improve and optimize the analysis method to optimize the analysis model.

Training model

The data analysis model of "smart parking" of big data is basically fixed. However, because the objects are different, the data parameters and elements selected are also different. By adjusting variables or elements to suit different requirements objects, the model becomes universal. The most appropriate parameters or variable elements are found through the training model, and the most appropriate model parameters are determined based on the real business data in intelligent parking.

Evaluation model

The specific data analysis model is evaluated under the business application scenario of government car yard supervision, and the common indicators to evaluate the model quality include average error rate and judgment coefficient. The commonly used indexes to evaluate the quality of classification prediction models include accuracy, recall, precision, ROC curve and AUC value.

Application model

After the evaluation and measurement of the data analysis model is completed, the model is applied to the practice of smart parking business to load the master data and subject data from the distributed data warehouse. Through data presentation and other means, the implicit information in various structured and unstructured data is displayed to solve the business problems in the work. So as to achieve the purpose of predicting the future development of parking lots.

Optimization model

In the evaluation data analysis model, if the model is found to be underfitting or overfitting, it indicates that the model needs to be optimized. In real application scenarios, optimization should be carried out regularly, or when it is found that the model does not work well in real business scenarios, optimization should also be started. Specific optimization measures can be considered to re-select the model, adjust model parameters, increase variable factors, etc.

4. Conclusions

In the whole research process, data collection and model construction are the most important two links. In the early stage of data collection, due to the different formats of data to be collected, a lot of data was lost in the collection process and a lot of dirty data also appeared. In the process of data acquisition in the later period, a unified data acquisition format should be formulated and data items that do not meet the requirements should be automatically filled or deleted in the collected data. Since big data technology is adopted, the speed of data collection is relatively critical. Considering that the amount of data will gradually increase in the later period, it is also noteworthy to improve the speed of data collection. In model construction, the combination of analysis elements is the most important, and the subsequent model design is set for the analysis of combination elements. Therefore, in the training and optimization of the model, more attention should be paid to the consistency of the selected analysis elements. Through the practice in the early stage, the intelligent parking construction in Tongliang District of Chongqing has been preliminarily improved, the chaotic data has been centralized managed, and the regulatory efficiency of the government has also been improved. The platform still needs to be improved in the future.

References

[1] A. Somani, S. Periwal, K. Patel and P. Gaikwad, "Cross Platform Smart Reservation Based Parking System," 2018 International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, 2018, pp. 1-5, doi: 10.1109/ICSCET.2018.8537282.

[2] T. Kiliç and T. Tuncer, "Smart city application: Android based smart parking system," 2017 International Artificial Intelligence and Data Processing Symposium (IDAP), Malatya, 2017, pp. 1-4, doi: 10.1109/IDAP.2017.8090284.

[3] J. Chen, Q. Jiang, Y. Wang and J. Tang, "Study of data analysis model based on big data technology," *2016 IEEE International Conference on Big Data Analysis (ICBDA)*, Hangzhou, 2016, pp. 1-6, doi: 10.1109/ICBDA.2016.7509810.

[4] L. Zheng, X. Xiao, B. Sun, D. Mei and B. Peng, "Short-Term Parking Demand Prediction Method Based on Variable Prediction Interval," in *IEEE Access*, vol. 8, pp. 58594-58602, 2020, doi: 10.1109/ACCESS.2020.2976433.

BRAIN TUMOR CLASSIFICATION USING EFFICIENT DEEP FEATURES OF MRI SCANS AND SUPPORT VECTOR MACHINE

AHMAD NEYAZ KHAN[1,2], HABIBEH NAZARIAN[3], NOORBAKHSH AMIRI GOLILARZ[1], ABDOLJALIL ADDEH[4], JIAN PING LI[1], GHUFRAN AHMAD KHAN[5]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China, [2] Department of Computer Application, MITS, A.P., India
[3] Department of Psychology, Yasuj Branch, Islamic Azad University, Yasuj, Iran
[4]Faculty of Electrical and Computer Engineering, Babol Noshirvani University of Technology, Babol, Iran
[5]School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China.
E-MAIL:ahmadnk500@gmail.com, nazaryan.h@gmail.com, noorbakhsh.amiri@std.uestc.edu.cn, jalil_addeh@yahoo.com, jpli2222@uestc.edu.cn, ghufraan.alig@gmail.com

Abstract:

Brain cancer is a life-threatening disease and hampers the normal operation of the human body. For correct diagnosis and methodical treatment planning, it is essential to detect the brain tumor in initial stages of development. This study proposes an intelligent diagnostic method for early detection of brain tumor. In the developed method, the deep features of magnetic resonance imaging (MRI) scans are used as the input of support vector machine (SVM). In the first step of the proposed method, Grab cut method is applied for segmenting tumor region, then the segmented images are fed to convolutional neural network (CNN) for deep feature extraction. Following feature extraction module, minimum Redundancy Maximum Relevance (mRMR) algorithm is used to select the most efficient deep features. Finally, the selected deep features are fed into SVM in the classification module. In addition, we applied the black widow optimization algorithm (BWOA) for optimal tuning of hyper-parameters of CNN and SVM. The developed method applied on BraTS 2015 datasets and the obtained results showed that the developed method is effective and may be employed in computer-aided diagnosis systems to classify the type of tumor.

Keywords:

MRI; Brain tumor; Feature extraction; mRMR; Deep learning

1. Introduction

The formation of abnormal groups of cells within the brain or near it results in the initialization of a brain tumor. The abnormal cells abrupt the processing of the brain and influence the wellness of a patient [1]. Glioma is a main brain tumor type and it has two classes including benign or Low Grade Glioma (LGG), and malignant or High Grade Glioma (HGG). As a rule, LGG tumors do not attack neighboring normal cells while HGG tumors strike on their near cells [2]. Therefore, accurate glioma identification and classification at its beginning phases is a serious necessity.

Recently, radiologists and clinicians to analyze brain tumors broadly utilize magnetic resonance imaging (MRI) scans. The MRI scans provides useful and important information connected to anatomical structures for planning treatment [3]. Radiologists still find it challenging to distinguish between LGG and HGG cells. Unfortunately, with a visual inspection, this suffers from the unavoidable human mistake and malfunction, which can be further amplified by noisy MR images. Furthermore, excellently trained algorithms in machine learning (ML) can concentrate on points that are not perceptible to the doctor's unaided vision, and therefore can serve to change such a perception.

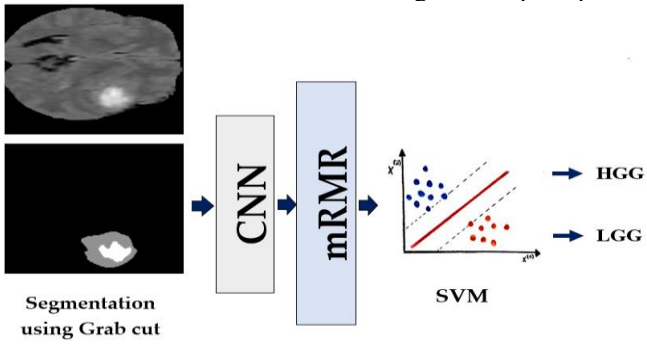


Fig.1 Main framework of the proposed brain tumor classification method

Over the past few years, ML-based approaches have become one of the leading research topics in medical image computing as well as in clinical diagnosis [4]. Such intelligent technologies also have great benefits over radiologists. They are reproducible, and hence they identify the subtle changes that visual observation cannot identify.

Over the past few years, several studies have been done on MR image processing using ML algorithms with the aim of providing an accurate brain tumor classification method. Most of the developed methods have used convolutional neural networks (CNN) as the classifier [5][6].

Considering the importance of early and accurate detection of brain tumor, a simple, fast and accurate diagnostic method is proposed in this study. In the developed method, we used CNN for automatic feature extraction from MR image slices. In order to improve the generalization capability, we used support vector machine (SVM) instead of fully connected layers (FCLs). Outstanding generalization capability of SVM makes it different from other classification algorithms.

Recently, neural networks, thresholding and optimization algorithms have been applied on various problems [8- 23]. In this research, black widow optimization algorithm (BWOA) is applied to find the optimal hyper-parameters of CNN and SVM. The BWOA is one of the most accurate and fast nature-based optimization algorithms that has been introduced recently [24]. For further improvement of recognition accuracy and reduction of computational burden, minimum Redundancy Maximum Relevance (mRMR) feature selection algorithm is implemented to select the most efficient deep features. The excellent performance of mRMR for feature selection is proved by different studies [25, 26]. The selected deep features are fed to SVM for final classification.

The rest of the article is arranged as follows. Section 2 presents the proposed method and provides details. In the third section, the results of numerical studies are presented. Section four summarizes and concludes the paper.

2. Proposed method

This paper proposes an intelligent method based on CNN and SVM for MR image analysis and brain tumor classification. The proposed method includes five main modules including the segmentation, feature extraction, feature selection, classification and optimization modules. Figure 1 shows the main framework of the proposed brain tumor classification method.

At the outset, RGB images are converted into a single channel. Subsequently, the Grab cut algorithm is implemented in the first module to segment and refine tumor region more correctly. The Grab cut is a powerful extension of the graph cut technique for segmentation of color images. In the feature extraction module of the proposed method, we used a CNN for generating deep and abstract features from segmented images that cannot be seen or detected by a human expert. The automatically extracted features lead to more accurate classification. In the feature selection module, mRMR algorithm is applied on extracted deep features by CNN. In the classifier module, we used SVM. The SVMs seem to be powerful alternatives to FCL, which overcome some of the basic weakness related to FCL while retaining all strengths of FCL [28].

One great obstacle for implementing any classifier on a new problem is that it requires the amount of considerable experience and skill to select fitting hyper-parameters. Since these hyper-parameters have internal relations, their tuning is notably expensive and time-consuming. These hyper-parameters in the developed classifier are number of convolution and pooling layer (NL), activation function type (T_{Act}), learning rate (ŋ), number of kernels in convolution layer (NK_C), size of kernels in convolution layer (SK_C), stride value in the convolution layer (S_C), zero-padding value (Z), pooling method type ($T_{pooling}$), size of kernels in pooling layer (SK_P), stride value in the pooling layer (S_P) in ConvNet, and gamma (γ) and penalty factor (PF) in SVM. In the developed method, we used Gaussian kernel function in SVM. The T_{Act} could be rectified linear unit (ReLU), randomized ReLU (RReLU) and parametric ReLU (PReLU) and the $T_{pooling}$ could be Mixed, L_P and Spatial Pyramid.

In the developed method, the BWOA is employed for finding the optimal value of hyper-parameters in CNN and the SVM network. In the propounded method, the first variable in each spider indicates the number of convolution-pooling layers in CNN, the second variable indicates the learning rate, and the third and fourth variables show γ and PF in the SVM. The reaming variables indicate the hyper-parameters of each convolution layer and the pooling layer. Eq. (1) shows a sample answer (spider) in the proposed method.

$$Spider = \begin{bmatrix} \text{NL} = 5, \quad \eta=0.0012, \quad \gamma=0.01 \quad \text{PF}=10 \\ T_{Act}^{1}, \ NK_{c}^{1}, \ SK_{c}^{1}, \ S_{c}^{1}, \ Z^{1}, \ T_{pool}^{1}, \ SK_{p}^{1}, \ S_{p}^{1} \\ T_{Act}^{2}, \ NK_{c}^{2}, \ SK_{c}^{2}, \ S_{c}^{2}, \ Z^{2}, \ T_{pool}^{2}, \ SK_{p}^{2}, \ S_{p}^{2} \\ T_{Act}^{3}, \ NK_{c}^{3}, \ SK_{c}^{3}, \ S_{c}^{3}, \ Z^{3}, \ T_{pool}^{3}, \ SK_{p}^{3}, \ S_{p}^{3} \\ T_{Act}^{4}, \ NK_{c}^{4}, \ SK_{c}^{4}, \ S_{c}^{4}, \ Z^{4}, \ T_{pool}^{4}, \ SK_{p}^{4}, \ S_{p}^{4} \\ T_{Act}^{5}, \ NK_{c}^{5}, \ SK_{c}^{5}, \ S_{c}^{5}, \ Z^{5}, \ T_{pool}^{5}, \ SK_{p}^{5}, \ S_{p}^{5} \\ \times \quad \times \quad \times \quad \times \quad \times \quad \times \quad \times \quad \times \\ \times \quad \times \quad \times \quad \times \quad \times \quad \times \quad \times \quad \times \end{bmatrix} \tag{1}$$

According to this spider, the formed ConvNet has five convolution-pooling layers; the learning rate is 0.0012, and second to sixth rows show the remaining hyper-parameters. For example, T_{Act}^{1} indicates the activation function type in the first convolution layer. The total number of hyper-

parameters in a CNN with five layers and SVM with two hyper-parameter is 44, $(4 + (5 \times 8) = 44)$. If the first variable of a sample spider is eight, then we will have eight convolution-pooling layers in ConvNet, and the total number of unknown hyper-parameters is 68, $(4 + (8 \times 8) = 68)$.

3. Results

The standard MRI benchmark datasets, Brain Tumor Segmentation (BraTS) 2015, is used to evaluate the performance of the developed brain tumor classification method. The BraTS 2015 Challenge dataset includes 384 cases such that 220 HGG and 54 LGG are in training and 110 of both (HGG, LGG) are in testing. The MRI cases have $(240 \times 240 \times 155 \times 4)$ dimension, where 155 shows the number of slices for each case and four shows the number of sequences [27]. Therefore, we have 33480 LGG and 136400 HGG slices in the training phase. In the testing phase, we used 8500 LGG slices and 41000 HGG slices. The simulations are performed using a personal computer with seven processing cores (core i7) and 16 GB RAM and Python programming language.

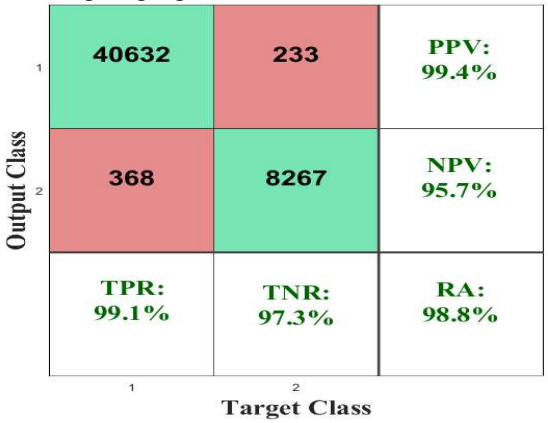


Fig.2 Performance of CNN - FCL

In the proposed method, hyper-parameters are selected using the optimization algorithm. In the BWOA, 30 spiders are generated randomly in the search space and the optimization process is iterated 100 times. Based on the best obtained results, SVM with Gaussian radial basis function (GRBF) led to the highest recognition accuracy. Therefore, we used this type of kernel function in the simulations. According to the BWOA, CNN with five layers (NL=5) and learning rate equal to 0.00128 ($\eta = 0.0028$) and SVM with $\gamma = 0.0812$ and PF= 42.6 lead to the best performance. In the developed method, 1400 deep features are extracted using CNN. In the following module, i.e. feature selection module, the most 241 efficient features are selected out of 4096 features using mRMR. The obtained results using different architectures are shown by Figures 2 to 5. In this figures, the performance of proposed method is shown in term of recognition accuracy (RA), sensitivity or true positive rate (TPR), specificity or true negative rate (TNR), precision or positive predictive value (PPV), and negative predictive value (NPV). For the all cases, the value of hyper-parameters is selected by BWOA.

For the first classifier (Fig 2), which uses the entire 4096 extracted deep features as the input of FCL, the value of RA is 98.76%. This values increase to 99.23% if we apply mRMR for feature selection. In this state, FCL uses the selected 241 efficient features as its input. The RA improvement indicates the high effect of feature selection. If we use SVM as the classifier and 241 features as it input (Fig 5), the value of RA enhances to 99.79%. It can be seen that the highest RA is achieved by the proposed methods (CNN –mRMR - SVM), which uses SVM as the classifier and selected deep features as the input vector.

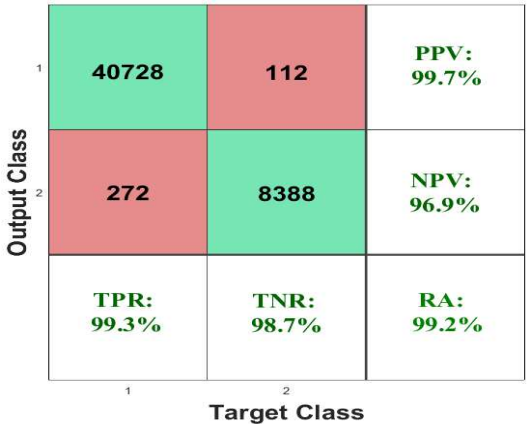


Fig.3. Performance of CNN - mRMR – FCL

4. Conclusion

In this study, a new hybrid method proposed for brain tumor detection and classification, and applied on BraTS 2015 dataset. In order to evaluate the performance of the developed method, several experiment was performed. In the first experiment, CNN followed by FLC are implemented for classification, and 98.76% accuracy achieved. In the next experiment, we used mRMR for feature selection, and the obtained results showed that feature selection has high effect on classification accuracy. Finally, we used SVM as the classifier and 241 selected deep features as its input vector. The obtained results showed that using efficient features and high performance classifier leads to highest accuracy, 99.79%.

References

[1] X. Wang, Y. Hu, R. Wang, P. Zhao, W. Gu, and L. Ye,"Albumin-mediated synthesis of fluoroperovskite KMnF3 nanocrystals for T1-T2 dual-modal magnetic resonance imaging of brain gliomas with improved sensitivity", Chemical Engineering Journal, Vol. 395, pp. 125066, 2020.

[2] M. A. Naser, and M. J. Deen, "Brain tumor segmentation and grading of lower-grade glioma using deep learning in MRI images", Computers in Biology and Medicine, Vol. 121, pp. 103758, 2020.

[3] S. K. Chandra, and M. K. Bajpai, "Fractional Crank-Nicolson finite difference method for benign brain tumor detection and segmentation", Biomedical Signal Processing and Control, Vol. 60, pp. 102002, 2020.

[4] S. Deepak, and P. M. Ameer, "Retrieval of brain MRI with tumor using contrastive loss based similarity on GoogLeNet encodings", Computers in Biology and Medicine, Vol. 125, PP. 103993, 2020.

[5] A. Ari, and D. Hanbay, "Deep learning based brain tumor classification and detection system", Turkish Journal of Electrical Engineering and Computer Sciences, Vol. 26, No. 5, pp. 2275- 2286, 2018.

[6] G. Martensson, and et al,"The reliability of a deep learning model in clinical out-of-distribution MRI data: A multicohort study", Medical Image Analysis, Vol. 66, PP. 101714, December 2020.

[7] P. Zarbakhsh, A. Addeh, and H. Demirel, "Early detection of breast cancer using optimized ANFIS and features selection," 9th International Conference on Computational Intelligence and Communication Networks (CICN), Cyprus, 2017.

[8] Abdoljalil Addeh, Aminollah Khormali, Noorbakhsh Amiri Golilarz. Control chart pattern recognition using RBF neural network with new training algorithm and practical features. ISA Transactions, 79 (2018) 202-216.

[9] Aminollah Khormali, Jalil Addeh. A novel approach for recognition of control chart patterns: Type-2 fuzzy clustering optimized support vector machine. ISA Transactions, 63 (2016) 256-264.

[10] J. Addeh, and A. Ebrahimzadeh, "Breast Cancer Recognition Using a Novel Hybrid Intelligent Method," Journal of Medical Signals and Sensors, vol. 2, pp. 22-30, 2012.

[11] A. Kalteh, P. Zarbakhsh, M. Jirabadi, and J. Addeh, "A research about breast cancer detection using different neural networks and K-MICA algorithm", Journal of Cancer Research and Therapeutics, Vol. 9, pp. 456- 466, 2013.

[12] J. Addeh, A. Ebrahimzadeh, and V. Ranaee. "Control Chart Pattern Recognition Using Adaptive Back-propagation Artificial Neural Networks and Efficient Features". 2nd International Conference on Control, Instrumentation and Automation (ICCIA), Shiraz, Iran, 2011 (IEEE, Citation: 11)

[13] J. Addeh, A. Ebrahimzadeh, and V. Ranaee. "Application of the PSO-RBFNN Model for Recognition of Control Chart Patterns". 2nd International Conference on Control, Instrumentation and Automation (ICCIA), Shiraz, Iran, 2011 (IEEE, Citation: 9)

[14] A. Khosravi, J. Addeh, and J. Ganjipour. "Breast Cancer Detection Using BA-BP Based Neural Networks and Efficient Features". 7th Iranian IEEE Conferences on Machine Vision and Image Processing (MVIP), Tehran, Iran, 2011.

[15] Spyrison (Spyros) Bakas. Brats MICCAI brain tumor dataset. IEEE Dataport, 2020 [Online]. Available: http://dx.doi.org/10.21227//hdtd-5j88. Accessed September 2020.

[16] N. Amiri Golilarz, H. Gao, and H. Demirel, "Satellite image De-noising with harris hawks meta heuristic optimization algorithm and improved adaptive generalized Gaussian distribution threshold function," IEEE Access, Vol. 7, pp. 57459–57468, 2019.

[17] M. Shahid et al., "Wavelet Based Image De-noising with Optimized Thresholding Using HHO Algorithm," 16th IEEE International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, pp. 6-12, 2019.

[18] N. Amiri Golilarz, A. Addeh, H. Gao, L. Ali, A. Moradkhani Roshandeh, H. Mudassir Munir, and R. U. Khan, "A New Automatic Method for Control Chart Patterns Recognition Based on ConvNet and Harris Hawks Meta Heuristic Optimization Algorithm," IEEE Access, Vol. 7, pp. 149398- 149405, 2019.

[19] N. Amiri Golilarz, H. Gao, R. Kumar, L. Ali, Y. Fu, C. Li, "Adaptive Wavelet Based MRI Brain Image De-noising," Frontiers in Neuroscience, Vol. 14:728, 2020.

[20] N. A. Golilarz and H. Demirel, "Image De-noising using Un-decimated Wavelet Transform (UWT) with Soft Thresholding Technique," Proceeding of IEEE CICN2017 Conference, pp. 16-19, September 2017.

[21] N. A. Golilarz, H. Gao, W. Ali, and M. Shahid, "Hyper-spectral remote sensing image de-noising with three dimensional wavelet transform utilizing smooth nonlinear soft thresholding function," in Proc. ICCWAMTIP, Chengdu, China, 2018, pp. 142-146.

[22] N. A. Golilarz et al., "Optimized wavelet-based satellite image de-noising with multi-population differential

evolution-assisted harris hawks optimization algorithm," IEEE Access, vol. 8, pp. 133076-133085, 2020.
[23] N. A. Golilarz, H. Demirel, and H. Gao, "Adaptive generalized Gaussian distribution oriented thresholding function for image de-noising," International Journal of Advanced Computer Science and Applications, vol. 10, no. 2, pp. 10-15, 2019.
[24] V. Hayyolalam, and A. Pourhaji Kazem, "Black Widow Optimization Algorithm: A novel meta-heuristic approach for solving engineering optimization problems", Engineering Applications of Artificial Intelligence, Vol. 87, pp. 103249, 2020.
[25] Y. A. Ahmed, B. Koçer, S. Huda, B. A. Saleh Al-rimy, and M. M. Hassan, "A system call refinement-based enhanced Minimum Redundancy Maximum Relevance method for ransomware early detection", Journal of Network and Computer Applications, Vol. 167, PP. 102753, October 2020.
[26] M. Toğaçar, B. Ergen, and Z. Cömert, "Detection of lung cancer on chest CT images using minimum redundancy maximum relevance feature selection method with convolutional neural networks", Biocybernetics and Biomedical Engineering, Vol. 40, No. 1, pp. 23-39, 2020.
[27] C. Rother, V. Kolmogorov, and A. Blake, ''-Grab Cut: interactive foreground extraction using iterated graph cuts", ACM Trans Graph, PP. 309-314, 2004.
[28] J. Gu, Z. Wang, J. Kuen, L. Ma, A. Shahroudy, B. Shuai, T. Liu, X. Wang, G. Wang, J. Cai, and T. Chen, "Recent advances in convolutional neural networks", Pattern Recognition, Vol. 77, pp. 354-377, 2018.

THE INFLUENCE MECHANISM OF STUDENTS' CONTINUOUS STUDYING INTENTION ON ONLINE EDUCATION LIVE-BROADCASTING PLATFORM

HUANG SIHAO[1], YE MENG[1], LI XINSHUO[2]

[1]Business School, Sichuan University, Chengdu 610065, China
[2]Chengdu Vocational&Technical College of Industry, Chengdu 610218, China
E-MAIL: 763974566@qq.com,2017225020025@stu.scu.edu.cn,1597335963@qq.com

Abstract:

Based on The ECM model, this paper explores the influencing factors and mechanism of students' intention to continue studying on the online education live-broadcasting platform. A total of 382 valid questionnaires were received through the online questionnaire interview, and the model and research hypothesis were analyzed through the structural equation Mplus7.4. The results show that perceived interactivity and perceived usefulness have significant positive effects on students' satisfaction. Both the expectation confirmation and the self-efficacy have positive effects on students' satisfaction. Students' satisfaction has a significant positive effect on their intention to continue studying.

Keywords:

Online education live-broadcasting platform; Perceived interactivity; Perceived usefulness; Satisfaction; Continuous studying intention

1. Introduction

With the continuous expansion of Internet technology and the gradual reduction of network bandwidth costs, the emerging model of the live-broadcasting has begun to integrate and develop with more industries. Education live-broadcasting has become an important part of the current era of online learning, especially in the context of COVID-19 sweeping the world this year. The Ministry of Education of China has put forward the guidelines of "no suspension of classes". The school has actively cooperated with the commercial platform to provide students with online learning resources. Among the many forms of online learning, many schools have chosen the method of online live-broadcasting. However, the survey found that students often "drop out of school" when they are online on the live-broadcasting platform, and it is difficult to concentrate for a long time. Therefore, in-depth research on the factors and mechanisms that affect students' continuous studying intention on the online live-broadcasting platform has become the key for schools to explore multiple teaching models and retain users on the platform. To increase students' participation in online classrooms and their continuous studying intention, the key is to understand what factors affect students' continuous studying intention? What are the internal mechanisms that affect students' continuous studying intention? And how should schools and platforms improve teaching methods and the experience of using live-broadcasting platforms in a targeted manner?

Therefore, this article is based on the ECM model, taking perceived interactivity, perceived usefulness, expectation confirmation and self-efficacy as antecedent variables, and satisfaction as an intermediary variable to establish a model of influencing factors of students' continuous studying intention on the online education live-broadcasting platform. The applicability of the ECM model is verified in the online education live-broadcasting platform scenario, and the study of learning behavior in the Internet field is expanded.

2. Research theory

The Expectation Confirmation Theory (ECT) was proposed by Oliver (1980), which believes that consumers will spontaneously form an expectation before consuming a certain product or service[1]. And after the actual use of the product or service, new feelings and cognition are generated, that is, perceived performance. Consumers will compare these two cognitions, and the resulting gap will further affect their subsequent continued buying behavior. This theoretical model has gradually been recognized by scholars and has become the basic theory for studying consumer satisfaction.

Expectation Confirmation Model is proposed by Bhattacherjee (2001) on the basis of expectation confirmation theory and technology acceptance model[2]. This model was later widely used to explain the continuous use behavior of information system users. Expectation confirmation is the gap between actual perceived performance and expectations. Satisfaction refers to a kind

of psychological state of users. The model believes that the user's expected confirmation will affect their perceived usefulness and satisfaction with the information system, and then affect their willingness to continue using it. The ECM model is universal and has been applied by scholars in the field of social psychology [3], e-commerce [4] and so on. Therefore, the ECM model can be well used in the study of the factors affecting the continuous studying intention of students on the online education live-broadcasting platform.

3. Research theory

(1) Perceived interactivity & satisfaction

The interactivity of the network platform can be divided into two types: actual interactivity and perceptual interactivity. Perceptual interactivity refers to a kind of subjective feeling of the user's interactive experience in the process of using the platform system [5]. Compared with the previous online learning platform, when students use the online education live-broadcasting platform for learning, they can communicate with teachers in time through barrage. Interactivity has become a major feature of the online education live-broadcasting platform. Students' perceptual interactivity in the platform can enhance their innovative spirit, thereby enhancing their flow experience [6]. Flow experience can generally generate the satisfaction. Chu and Yuan further pointed out that the user's perceptual interactivity in the network platform can help them generate positive emotions for the platform, and ultimately produce satisfaction[7].

Therefore, this article proposes the following assumption:

H1: *Students' perceived interactivity significantly positively affects their satisfaction.*

(2) Perceived usefulness & satisfaction

Perceived usefulness refers to the degree of user trust in the platform system to improve their work performance [8]. The perceived usefulness of users in the knowledge community can effectively promote knowledge search and sharing behavior, so as to obtain a better learning experience. Students can get an immersive learning experience through online knowledge sharing during the learning process of the online education live-broadcasting platform. Kim et al. pointed out that the perceived usefulness of smartphone users for emerging technologies can positively affect their satisfaction. Therefore, this article proposes the following assumption:

H2: *Students' perceived usefulness significantly positively affects their satisfaction.*

(3) Expectation confirmation & satisfaction

Expectation confirmation is the perception evaluation made by users after using the network platform system. Scholars have confirmed that the user's expectation confirmation of the network platform system is the core element of shaping their satisfaction [9]. The students' evaluation of the online education live-broadcasting platform comes from actual experience. Due to the outstanding interface experience and timely updates of the platform, the user experience is often higher than their expectations, and the final evaluation of the online education live-broadcasting platform by users is often more positive and satisfactory. Therefore, this article proposes the following assumption:

H3: *The expectation confirmation of students significantly positively affects their satisfaction*

(4) Self-efficacy & satisfaction

The self-efficacy in the computer field refers to the user's assessment of the personal abilities required to use computers and related systems [10]. Individuals with a high degree of self-efficacy are often able to mobilize their initiative and other related resources to accomplish their goals. In the online learning process, when a student actively participates in a live-broadcasting classroom, he can obtain a wealth of learning resources, which is conducive to completing the learning goals and ultimately improving his satisfaction. Therefore, this article proposes the following assumption:

H4: *Students' self-efficacy significantly positively affects their satisfaction.*

(5) Satisfaction & continuous studying intention

User satisfaction refers to the overall assessment of the achievement of its established goals and the degree of satisfaction of needs, which can better explain the user's behavioral wishes. Therefore, satisfaction is an important psychological internal state when studying user behavior intentions. Cheng's research found that in the field of online learning, user satisfaction is the biggest influencing factor of their willingness to continue using [11]. Cao Gaohui pointed out that satisfaction plays a mediating role between perceived usefulness, expectation confirmation, and intention to continue participation[12]. Therefore, the following assumption is made:

H5: *Student satisfaction significantly positively affects Continuous Studying Intention.*

Based on the above analysis, the research model in this paper is shown in fig.1.

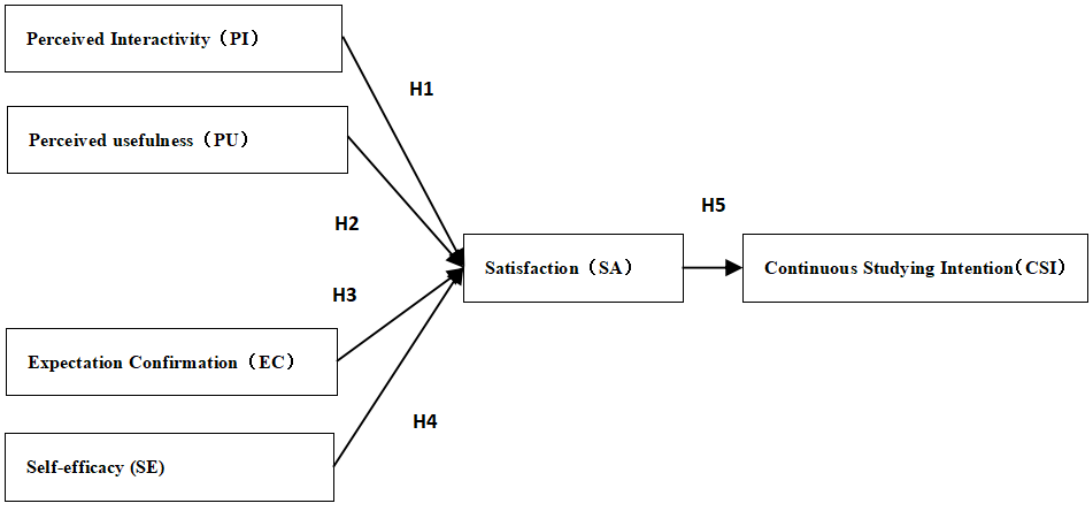


Fig.1 Conceptual model of the influence mechanism of students' CSI on the online education live-broadcasting platform

4. Research methods and result analysis

4.1. Questionnaire design and data collection

The questionnaire in this article is mainly divided into two parts, the first part is demographic variables, and the second part is research variables. The research variables were measured using Likert 5-level scale. The values from 1-5 represent the change from completely disagree to completely agree. Perceived Interactivity (PI) refers to the scale of [13], with a total of 4 items. Perceived usefulness refers to the scale of [14] and [15], with 4 items in total. Expectation confirmation (EC) refers to [2], with a total of 3 items. Self-efficacy (SE) refers to [16], with a total of 3 items. Satisfaction (SA) refers to the scale of [17], with a total of 3 items. Continuous Studying Intention (CSI) refers to [2], with a total of 3 items. The detailed description and reference of the scale are shown in Table 1.

Table 1 Questionnaire items

Variable	Indicator code	Measurement item
PI	PI1	When watching the teacher's live - broadcasting lecture, the communication and interaction methods between the teacher and the students are very diverse.
	PI2	While watching the teacher's live - broadcasting lecture, I was able to communicate and interact with the teacher in a timely manner.
	PI3	While watching the teacher's live - broadcasting lecture, I was able to communicate and interact with other students in a timely manner.
	PI4	While watching the teacher's live - broadcasting lecture, I can send bullet screens to ask questions.
PU	PU1	Using the online education live - broadcasting platform helps me get a better online learning experience.
	PU2	Using the online education live - broadcasting platform helps me improve my academic performance.
	PU3	Using the online education live - broadcasting platform helps me improve my learning efficiency.
	PU4	The online education live-broadcasting platform can provide me with valuable information or services.
EC	EC1	The experience I have gained in using the online education live-broadcasting platform has exceeded my expectations.
	EC2	The quality of the online education live - broadcasting platform system I used exceeded my expectations.
	EC3	Most of my expectations for the online education live-broadcasting platform have been fulfilled.
SE	SE1	I have the knowledge and skills to use the online education live-broadcasting platform.
	SE2	Even if there is no one to assist or supervise me, I have the confidence to use the online education live-broadcasting platform.
	SE3	Even if I have never used a similar online learning platform, I am confident to use the online education live-broadcasting platform.
SA	SA1	I think it makes sense to participate in live-broadcasting learning.
	SA2	The process of participating in the online

		live-broadcasting learning made me feel satisfied.
	SA3	I am satisfied with the results of participating in the live-broadcasting learning.
CSI	CSI1	I will continue to conduct online learning on the online education live - broadcasting platform in the future.
	CSI2	I would like to recommend my friends to use the online education live - broadcasting platform.
	CSI3	Even if there are other online learning platforms, I am willing to continue to use the online education live-broadcasting platform.

In order to ensure high-quality survey data, this study mainly uses online questionnaires for data collection, and the effective respondents are students who have used the online education live-broadcasting platform. In the preliminary analysis of the questionnaire results, in order to avoid statistical errors, the questionnaire with the same answer to multiple consecutive questions will be regarded as invalid. According to statistics, this round of pre-surveys distributed research questionnaire samples to 120 audiences, and recovered 107 valid questionnaires, with an effective rate of 89.17%. Reliability and validity analysis of the recovered questionnaire data found that the reliability test value of Cronbach's α of each scale is greater than 0.70, and the KMO value of each scale is also greater than 0.70. This shows that the reliability and validity of the questionnaires used are all at a high level and can be used for formal investigations. A total of 430 questionnaires were collected during the formal investigation process of this study. After excluding invalid questionnaires, 382 valid questionnaires were obtained, and the effective rate was 88.84%. The distribution of the sample of interviewees in the formal survey is as follows: The proportion of female samples is 48.95%; 20.16% of the interviewees are between 13-15 years old,62.57% of the interviewees are between16-18 years old,7.07% of the interviewees are between19-22 years old,5.76% of the interviewees are between 23-26 years old,the rest are over 26 years old; most of them are high school students, 15.57% of interviewees are college students.

4.2. Reliability and validity analysis

This study uses SPSS 25.0 to conduct statistical analysis on the primary data collected in the formal survey. This paper is a Likert 5-level scale, using Cronbach's α coefficient to test the reliability of 6 latent variables and 20 measurement items respectively to evaluate the internal consistency of the scale. At the same time, the validity of the scale is judged according to the standardized load of each observation item, the combined reliability of the scale and the average extracted variation. As shown in the reliability and validity analysis of Table 2, the minimum value of the standardized factor load of each measurement item under each variable is 0.808, which is greater than the threshold value of 0.5. The CR values of the combined reliability coefficients were all greater than 0.7, and the average variance extraction AVE values were all greater than 0.5. It shows that each measurement item in the scale can significantly affect the corresponding latent variable, and the aggregation validity of each latent variable is good. The Cronbach's α of all variables is greater than the accepted reliability standard of 0.7, indicating that the reliability of the scale is high and the scale has good internal consistency.

Table 2 Statistical table of reliability and validity of variables

Index	Item	Standardized factor loadings	Cronbach's α	*CR*	*AVE*
PI	PI1	0.838	0.944	0.918	0.738
	PI2	0.895			
	PI3	0.891			
	PI4	0.808			
PU	PU1	0.904	0.967	0.952	0.831
	PU2	0.929			
	PU3	0.932			
	PU4	0.881			
EC	EC1	0.934	0.966	0.956	0.878
	EC2	0.952			
	EC3	0.924			
SE	SE1	0.874	0.942	0.925	0.805
	SE2	0.880			
	SE3	0.936			
SA	SA1	0.909	0.956	0.942	0.844
	SA2	0.922			
	SA3	0.925			
CSI	CSI1	0.924	0.961	0.949	0.861
	CSI2	0.908			
	CSI3	0.951			

In this study, the method of competitive substitution model was used to carry out confirmatory factor analysis to further illustrate the discriminative validity between variables. According to the connotation and statistical requirements of each variable, this study puts forward 6 competitive models, and uses RMSEA, CFI, TLI, SRMR and other indicators for judgment. According to the results in Table 3, the result of the seven-factor model is the best：x^2 (114) =496.339($p<0.001$)， CFI=0.971， TLI=0.961， RMSEA=0.067，SRMR=0.042. Other competitive models are inferior to the six-factor model. The above test shows that the six variables in this study have good discriminative

validity

Table 3 Confirmatory factor analysis results

Model	x^2	*df*	x^2/df	$\triangle x^2$(*df*)	CFI	TLI	RMSEA	SRMR
Six-factor model	1076.29	155	6.94	-	0.921	0.903	0.125	0.035
Five-factor model	1376.56	160	8.60	1.66	0.896	0.876	0.141	0.034
Four-factor model	1529.78	164	9.33	2.39	0.883	0.864	0.148	0.033
Three-factor model	1866.33	167	11.18	4.24	0.854	0.834	0.164	0.036
Two-factor model	2056.93	169	12.17	5.23	0.838	0.818	0.171	0.039
One-factor model	2111.03	170	12.42	5.48	0.834	0.814	0.173	0.039

Note：Six-factor model = PI,PU,CO,SE,SA,CSI ;Five-factor model=PI+PU,CO,SE,SA,CSI; Four-factor model= PI +PU +CO,SE,SA,CSI; Three-factor model=PI + PU,SE+ SA,CO +CSI; Two-factor model=PI +CO +SA +CSI,PU +SE; One-factor model=PI+PU+CO+SE+CSI.N=382,***stands p<0.001（two-tailed test）

4.3. Model hypothesis testing

This article uses Mplus7.4 to construct a structural equation model and test the basic hypothesis. The results of the study are shown in Table 4.

Table 4 Research hypothesis test results

Hypothesis	Path	*β*	*SE*	*P value*	Support
H1	PI→SA	0.926	0.047	0.000	valid
H2	PU→SA	0.880	0.037	0.000	valid
H3	EC→SA	0.807	0.033	0.000	valid
H4	SE→SA	0.859	0.040	0.000	valid
H5	SA→CSI	0.886	0.030	0.000	valid

Note: ***p＜0. 001. *SE* = standard error

5. Conclusion and Implication

5.1. Conclusion

(1) Students' perceived interactivity and perceived usefulness have a significant positive impact on their satisfaction.

From the perspective of users' experience of using information systems, the operability, interactivity, and value of current network platforms have become important dimensions for users to perceive and evaluate the quality of the platform, and to generate user satisfaction. When students are learning through online live-broadcasting content, the online social experience obtained on the platform represents their perceived interactivity. At the same time, when students use the online education live-broadcasting platform, their perception of interface operability and the learning value gained after learning represent the overall evaluation of their perceived usefulness. This proves that students' perceived interactivity and perceived usefulness can promote their satisfaction with the online education live-broadcasting platform.

(2) Students' self-efficacy and expectation confirmation have a significant positive impact on their satisfaction.

Self-efficacy is an influential factor in students' use of information technology in the field of perceptual behavior control, and the degree of expectation confirmation is the overall evaluation of users after using the system. The results demonstrate that both platform and teacher should help students improve their level of self-efficacy and expectation confirmation as to improve the positive attitude and satisfaction.

（3）Satisfaction has a significant positive impact on the Continuous Studying Intention.

Some scholars have proved that satisfaction in the field of information systems is an important factor influencing users' willingness to continue to use. The satisfaction of students with the online education live- broadcasting platform represents the positive feedback of the overall use. The positive psychological feedback mechanism will further promote the willingness to continue learning. Therefore, it is especially important to maintain students' high satisfaction and positive evaluation of the platform and learning effect when students are learning online.

5.2. Implication

In the post-epidemic era, normalized online teaching will become a common form of teaching, and how to improve students' continuous studying intention is an important research direction. Therefore, this article puts forward the following practical suggestions through the research results:

Firstly, optimize the design of online education live-

broadcasting platform and enrich course content. The platform needs to further optimize its functional layout, make the navigation functions in the platform clearer to improve student search efficiency, and make interactive functions and tools more concise and convenient to provide students with a better real-time interactive experience. The platform also needs to adjust its course design according to the student's learning behavior data to further enrich the content of the online course that students need and are interested in. Enhance students' perceived usefulness with rich course content.

Secondly, teachers and platforms should work together to cultivate students' online learning ability and enhance students' self-efficacy in information systems. The platform should create a more realistic learning scene. At the same time, teachers should cultivate students' ability to quickly search for learning resources and use various learning tools flexibly. Only when students fully master various learning techniques can their sense of self-efficiency be further improved.

Thirdly, teachers and parents should jointly cultivate students' self-supervision ability. Teachers should guide students to plan online learning goals and achieve timely feedback through remote communication. At the same time, teachers should formulate a suitable evaluation system based on the characteristics of online learning to motivate students to complete their learning goals. Parents should also strengthen the supervision and support of students in the learning process at any time to enable them to successfully complete their goals. The achievement of students' learning goals is conducive to the realization of self-expectations and can further shape their independent learning ability.

5.3. Limitations and future research

The further research of this article is as follows: Firstly, the factors affecting student satisfaction and continuous studying intention need to be expanded. The influencing factors of students' willingness to continue learning and satisfaction can be researched and expanded from different theoretical perspectives for example the TAM model. Because, this article only examines its influencing factors from the perspective of the expectation confirmation model. Secondly, follow-up research can consider more direct methods such as web crawler technology to obtain objective data of users and to gain more insights.

Acknowledgements

This paper is supported by the National Social Science Fund of China (20BGL268).

References

[1] Oliver, R.L. A cognitive model of the antecedents and consequences of satisfaction decisions, Journal of marketing research, Vol 17,No. 4, pp. 460-469, 1980.

[2] Bhattacherjee, A. Understanding information systems continuance: an expectation-confirmation model, MIS quarterly, Vol 351-370, 2001.

[3] Hossain, M.A. and M. Quaddus, Expectation–confirmation theory in information system research: A review and analysis, in Information systems theory. Springer. p. 441-469, 2012.

[4] Junjun, L., G. Dongxiao, and C. Yuanyuan. User behavior model and empirical research based on experience process, Information Science, Vol 37,No. 4, pp. 44-51, 2019.

[5] Voorveld, H.A., P.C. Neijens, and E.G. Smit. The Relat ion Between Actual and Perceived Interactivity, Journal of Advertising, Vol 40,No. 2, pp. 77-92, 2011.

[6] Rodríguez-Ardura, I. and A. Meseguer-Artola. E-learning continuance: The impact of interactivity and the mediating role of imagery, presence and flow, Information & Management, Vol 53,No. 4, pp. 504-516, 2016.

[7] Chu, K.-M. and J. Yuan. The effects of perceived interactivity on e-trust and e-consumer behaviors: The application of fuzzy linguistic scale, Journal of Electronic Commerce Research, Vol 14,No. 1, pp. 124, 2013.

[8] Davis, F.D., R.P. Bagozzi, and P.R. Warshaw. User acceptance of computer technology: a comparison of two theoretical models, Management science, Vol 35,No. 8, pp. 982-1003, 1989.

[9] Kim, B. and I. Han. The role of trust belief and its antecedents in a community-driven knowledge environment, Journal of the American Society for Information Science and Technology, Vol 60,No. 5, pp. 1012-1026, 2009.

[10] Bandura, A. Social foundations of thought and action, Englewood Cliffs, NJ, Vol 1986,No. 23-28, 1986.

[11] Cheng, Y.-M. Extending the expectation-confirmation model with quality and flow to explore nurses' continued blended e-learning intention, Information Technology & People, 2014.

[12] Gaohui, C., et al. An Empirical Study on Consumers' Willingness to Continue Participating in Online Reviews, Management Review, Vol 29,No. 11, pp. 148-158, 2017.

[13] Wei, X., W. Shupan, and P. Qiong. Research on the Influence of WeChat Mobile Social User's Flow Experience on User Stickiness, The Press, Vol 7, pp. 13-

18, 2015.
[14] Davis, F.D. Perceived usefulness, perceived ease of use, and user acceptance of information technology, MIS quarterly, Vol 319-340, 1989.
[15] Guritno, S. and H. Siringoringo. Perceived usefulness, ease of use, and attitude towards online shopping usefulness towards online airlines ticket purchase, Procedia-Social and Behavioral Sciences, Vol 81,No. 212-216, 2013.
[16] Igbaria, M. and J. Iivari. The effects of self-efficacy on computer usage, Omega, Vol 23,No. 6, pp. 587-605, 1995.
[17] Valvi, A.C. and D.C. West. E-loyalty is not all about trust, price also matters: extending expectation-confirmation theory in bookselling websites, Journal of Electronic Commerce Research, Vol 14, No. 1, pp. 99, 2013.

LARGE-SCALE FACE IMAGE RETRIEVAL BASED ON HADOOP AND DEEP LEARNING

HUANG YUANYUAN[1, 2], TANG YUAN[1, *], XIONG TAISONG[1, 2, *]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China
[2]Chengdu University of Information Technology, Chengdu, 610225, China
E-MAIL: iyyhuang@hotmail.com, tangyuanmail@gmail.com, xiongtaisong@gmail.com

Abstract:

In this paper, we analyzed large-scale face image retrieval method in cloud computing environment. Based on Hadoop platform, a large-scale face retrieval method by using deep learning was established to take advantage of parallel computing of MapReduce, and thus improving the efficiency of facial image retrieval. This method uses Histogram of Oriented Gradients and adopts a deep residual network. Meanwhile, Hadoop was adopted to process data parallelly to improve the retrieval efficiency. CASIA WebFace dataset was chosen for testing the proposed method, and the results of the experiment could demonstrate the effectiveness of the new method.

Keywords:

Face image retrieval; Hadoop; HOG; Deep learning

1. Introduction

With the rapid development of information technology, face recognition has been widely used in our daily life [1]. In the meantime, image retrieval has become an active topic in the field of computer vision and image understanding. Specifically, facing with the large-scale size of the image resource, how to accurately and quickly retrieve the image information from the large-scale image database becomes a very practical subject. Therefore, researchers and engineers begin to pay more and more attention to massive image retrieval with the emergence of large-scale data. As one of the most important applications in CBIR, face image retrieval, which is a difficult and cutting-edge problem, has very important research value. Different from face recognition, face image retrieval is composed of several steps including face detection, feature extraction and matching in large-scale datasets [4]. In the era of big data, this kind of similar face retrieval technology has a wide range of application value in the fields of video surveillance, human-computer interaction, biometrics security, military and Internet of Things, etc. [2-4,11]. However, with the increasing amount of face image data, the traditional face image processing technology in stand-alone mode cannot meet the needs of users [2].

In recent years, cloud computing technology could efficiently integrate available distributed computing resources in networks and complete the calculation task [1]. Therefore, the face image retrieval system based on distributed technology has become a research hotspot in recent years. In 2017, Zhang [2] design and realization of face image retrieval system based on spark framework. In 2019, Zhang [1] proposed a Distributed SVM face recognition based on Hadoop. Wang et al. proposed a large-scale real-time face retrieval system based on storm [4].

In this paper, we combine the face recognition via deep learning and cloud computing to solve the problems in large-scale face image retrieval. Firstly, we adopt a face detection model by using Histogram of Oriented Gradients (HOG) [5-6] and Support Vector Machine (SVM) [1,7]. Second, we use deep residual network [8] in face recognition. Then, we implement the face image retrieval based on Hadoop and MapReduce parallel computing model [9]. Since face feature extraction and face image retrieval was implemented on the Hadoop platform to take the advantages of the parallel computing of MapReduce, it can greatly improve the efficiency of face image retrieval. Finally, we use CASIA WebFace dataset [10] for testing and the results of the experiment could demonstrate the effectiveness of the new method. Our method has following advantages:

(1) The proposed method can merge the image feature files and store them in the Hadoop Distributed File System (HDFS) to speed up the storage and reading of massive image data in that face image feature files are very small.

(2) As the face image data set and features are stored in the HDFS file system, face image retrieval adopting MapReduce parallel computing framework makes use of the advantages of parallel computing to improve the efficiency greatly.

(3) The method adopts HOG and SVM in face detection and uses deep residual network for face recognition, this can

guarantee the Precision of face image retrieval.

The paper is organized as follows: In section two, we will give brief introductions of some related key technologies. In section three, our large-scale face image retrieval framework is proposed, and the experiment results are summarized in section four, followed by the discussions and conclusions in Section five.

2. Related key technologies

Generally, face image retrieval needs to implement face detection, feature extraction and matching in related datasets. The large-scale face image retrieval framework proposed in this paper is mainly based on some key technologies. So, we will briefly introduce these technologies below, including face detection using Histogram of Oriented Gradients and SVM, Face recognition by using Deep Residual Network, and Hadoop and its applications in our work.

2.1. Face detection using histogram of oriented gradients and SVM

In our large-scale facial image retrieval framework, we firstly adopt a face detection model based on the combination of Histogram of Oriented Gradients (HOG) [5-6] and Support Vector Machine (SVM) [1,7]. After the feature extraction from the image, the problem whether the image contains a face is converted into a binary classification problem, and thus the detection results could be obtained by using SVM classifier. Here we give a brief description of calculation of HOG. The HOG feature descriptor which could describe local object appearance and shape within an image by the distribution of intensity gradients or edge directions, is prevalent in object detection and classification [5]. The details of the HOG calculations are described as below.

Suppose $I(x, y)$ denotes the pixel intensity at the position (x, y) in a image, $f_x(x, y)$ and $f_y(x, y)$ denote x and y components of the image gradient, which could be calculated through equation(1).

$$\begin{cases} f_x(x, y) = I(x+1, y) - I(x-1, y) \forall x, y \\ f_y(x, y) = I(x, y+1) - I(x, y-1) \forall x, y \end{cases} \quad (1)$$

And the magnitude m(x, y) and orientation θ(x, y) can be calculated through equation (2).

$$\begin{cases} m(x, y) = \sqrt{f_x(x, y)^2 - f_y(x, y)^2} \\ \theta(x, y) = \tan^{-1}(f_y(x, y) / f_x(x, y)) \end{cases} \quad (2)$$

Then, the gradient image can be divided into many cells. In each cell, the orientation θ(x, y) could be quantized into orientation bins, weighted by its magnitude m(x, y) to make the histogram. Finally, the block normalization could be done to get the HOG features [6].

2.2. Face recognition by using deep residual network

After the face detection, the face recognition technology in our work adopts deep residual network (ResNet) [8]. The deep residual network, as shown in figure 1, is a new type of specialized neural network, and it can handle many sophisticated deep learning tasks.

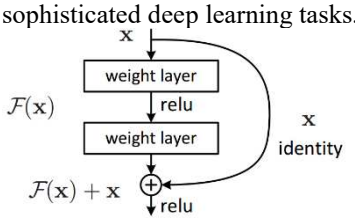


Fig.1 A building block in ResNet [8]

In our work, the face image could be transformed into high dimensional feature vector. The facial feature extraction can be realized by a job of MapReduce to improve the efficiency and the features are stored in Hadoop distributed file system.

2.3. Face image retrieval based on Hadoop and MapReduce parallel computing

In recent years, Hadoop has become a new standard for massive data storage and processing, and MapReduce has been the parallel programming model of Hadoop because it can take full advantage of the computing resources of each cluster to efficiently process the stored data [1,9]. In this paper, the proposed method could store a large number of face images in the HDFS. With the increase of the number of face images, the time used for feature extraction based on Hadoop grows very slowly, while that of single machine increases very fast. Therefore, the feature extraction based on Hadoop has a great improvement compared with feature extraction on single machine. Besides, face image retrieval based on MapReduce parallel computing framework could retrieve the data sets parallelly to improve the retrieval efficiency. These tasks could be done by using MapReduce Job.

3. Large-scale face image retrieval framework

Based on the above technologies, we proposed a new large-scale face image retrieval framework. First, we use a

face detection model based on HOG and Support Vector Machine to get the position of the face in the origin image. Second, the face features are extracted through the model of deep residual network and it can transform the face into high dimensional feature vector which can be saved in HDFS. Third, the face image retrieval task can be accomplished based on Hadoop and MapReduce parallel computing. Therefore, the framework of the new large-scale face image retrieval including three main parts [3]:

(1) Face image data processing subsystem. For a given face image set, it is necessary to merge a large number of small files into a sequence file and store them in the HDFS due to the low performance of Hadoop framework for a large number of small files. Then, the features of each face image are extracted by MapReduce job and converted into a high dimensional feature vector set and stored in HDFS.

(2) Feature matching subsystem. This subsystem firstly extracts the feature vector of the face to be retrieved, and then try to get the retrieved result.

(3) User interaction subsystem. This subsystem is used to deal with human-computer interaction routine, present the retrieval results and count the total time spent in the retrieval process.

On the one hand, because HDFS of Hadoop is used for storage and MapReduce parallel computing framework is adopted, the proposed approach should have good fault tolerance and scalability, and it makes use of the advantages of parallel computing to improve the efficiency of face feature extraction and face image retrieval. On the other hand, the precision of face image retrieval can be guaranteed in that deep learning-based face recognition has been proved to be the most effective technology in recent years. Thus, the new approach could effectively improve the performance of large-scale face image retrieval.

4. Experiment and performance evaluations

In the experiment, Hadoop cluster is composed of three computers, one master, two slaves. The operating system is Centos 7.3. The Hadoop version is 2.6.5. The cluster configuration information is listed in table 1.

Table 1 Hadoop cluster configuration information

machine	OS	CPU	memory
master	Centos7.3	i7-8700T	8G
slave1	Centos7.3	Pentium(R)G3260	8G
slave2	Centos7.3	Pentium(R)G3260	8G

We choose CASIA WebFace dataset for testing. The face images in CASIA WebFace Dataset are collected from the Internet. It is a large-scale dataset which contains about 10,000 subjects and 500,000 images [10]. The face image retrieval in large-scale datasets were done for 10 times. The most commonly used indicators in image retrieval including precision, recall and time are recorded in table 2.

Table 2 Large-scale face image retrieval results

Number	Precision	Recall	Time(s)
1	86.36%	86.36%	32.15
2	93.55%	67.44%	31.01
3	100.00%	66.67%	48.11
4	100.00%	54.55%	37.46
5	100.00%	82.89%	34.69
6	100.00%	73.33%	38.25
7	66.67%	53.85%	38.42
8	100.00%	33.33%	30.77
9	86.66%	72.22%	43.52
10	83.33%	60.60%	35.02
Average	91.66%	65.12%	36.94

From table 2, we can get that average precision is 91.66% and average recall rate is 65.12%, and the whole system can provide second responsiveness for a majority of test conditions. Moreover, due to the use of Hadoop cluster, it has good scalability and fault tolerance. The results of the experiment could demonstrate that the effectiveness of the method in this paper.

5. Conclusions and future work

Nowadays, large-scale face image retrieval has broadly applications and important research value. In this paper, we mainly investigate the impact of Hadoop for large-scale face image retrieval. Moreover, we adopt HOG for face detection and ResNet for face recognition. However, this work is very preliminary, so we will continue to study the Hadoop and MapReduce parallel computing model and its applications in large-scale face image retrieval. Besides, we will try to use other large-scale face datasets for testing.

Acknowledgements

This paper is supported in part by the Sichuan Science and Technology Program under Grants 2018RZ0072, 2019YFS0068 and 20ZDYF0660, in part by the Foundation of Chengdu University of Information Technology under Grant J201707, in part by the College Students' innovation project of Chengdu University of Information Technology under Grant 202010621268.

References

[1] B. Zhang, “Distributed SVM face recognition based on Hadoop”, Cluster Computing, No.22, pp. S827-S834, 2019

[2] L. Zhang, F. Huan, Y. Wang, “Parallel image processing implementation under Hadoop cloud platform”, Information Security and Communications Privacy, No.10, pp.59-62, 2012
[3] A. Zhang, “Design and realization of face image retrieval system based on spark framework”, Xi’an: Northwest University, 2017
[4] C. Wang, C. Fan, Y. Wu, “Large-scale real-time face retrieval system based on Storm”, Computer Systems and Applications, No.3. pp.93-98,2019
[5] N. Dalal, B. Triggs, “Histograms of oriented gradients for human detection”, IEEE Conference on Computer Vision and Pattern Recognition, pp. 886-893, 2005
[6] Y. Huang, H. Yang, P. Huang. “Action recognition using HOG feature in different resolution video sequences”, International Conference on Computer Distributed Control and Intelligent Environmental Monitoring, Zhangjiajie, 2012, 85-88
[7] Y. Huang, D. Wang, Y. Sun, et al. “A fast intra coding algorithm for HEVC by jointly utilizing naive Bayesian and SVM”, Multimedia Tools and Applications,2020
[8] K. He, X. Zhang, S. Ren, et al. “Deep residual learning for image recognition”, IEEE Conference on Computer Vision and Pattern Recognition, pp.770-778, 2016
[9] R. Li, H. Hu, H. Li, et al, “MapReduce parallel programming model: a state-of-the-Art survey”, International Journal of Parallel Programming. 2015
[10] Y. Dong, Z. Lei, S. Liao, et al, “Learning face representation from scratch”, Computer science, 2014.
[11] J. Khan, J. Li, B. Ahamad, et al, “SMSH: secure surveillance mechanism on smart healthcare IoT system with probabilistic image encryption”, IEEE Access, Vol.8, pp.15747-15767,2020

INDIVIDUALIZED NEUROMARKERS TRACK MULTIPLE SYMPTOM DOMAINS IN EARLY-ONSET SCHIZOPHRENIA

FAN YUN-SHUANG[1], LI HAORU[1], LI LIANG[1], SHENG WEI[1], WANG CHONG[1], CHEN HUAFU[1*]

[1]The Clinical Hospital of Chengdu Brain Science Institute, University of Electronic Science and Technology of China, Chengdu, China

E-MAIL: fmrifanys@163.com, lihaoru001@163.com, liliang_hust@163.com, acca.swei@gmail.com, vincenzo1994@163.com, *chenhf@uestc.edu.cn

Abstract:

Neuroimaging-based biomarkers at individual level have promising potential to redefine psychiatric diseases as neural circuit disorders. In this study, a reliable cortical parcellation approach was used to map individual-specific functional connectome markers underlying multiple symptom domains in 39 patients with early-onset schizophrenia. Positive symptom burden could be predicted by a set of frontoparietal-based connections; and depression domain could be estimated by another distinct functional connectome among individually specified brain regions. The novel findings reveal dimension-specific individualized functional connectome markers in early-onset schizophrenia. More broadly, the current study may promote future development of personalized treatment strategies.

Keywords:

Biomarkers; Early-onset; Individualized; Neuroimaging; Schizophrenia

1. Introduction

Neuroimaging marker holds excellent promise for the current diagnosis, prognosis, and treatment of complex psychotic disorders, especially schizophrenia. These psychiatric patients may be unable to portray their heterogenetic symptom burdens. As an indicator of neuronal function, brain-based neuromarker could provide an objective measure of patient's pathological states. Furthermore, it can be used to determine if therapeutic candidates evoke their targeted biological effects [1]. With recent advances in functional neuroimaging, connectome-based biomarkers could be promising candidates for psychotic disorders [2]. For example, functional connectome (FC) markers have been identified to monitor cognitive and social deficits in schizophrenia, that can inform the treatment of cognitive dysfunction [3]. Therefore, we inferred that individualized FC-based markers have the potential to track the effect of treatment with psychotropic agents at the individual level in future research. However, individualized neuromaker remains poorly studied.

Personal characteristics are likely derived from the organization heterogeneity of brain functional systems across individuals [4-5]. For instance, individual variation in the size, location, and connectome of brain functional areas were proved to offer nonredundant information on human behaviors [6]. Recently, a novel cortical parcellation strategy that accounts for individual variability in brain functional systems was proposed to capture distinct features across individuals [7]. Individualized FC calculated by this method have been identified as reliable neuromarkers of symptom burden in multiple psychiatric disorders [8-9].

In this study, we adopted the cortical parcellation approach to map individual-specific functional brain networks in 39 first-episode early-onset schizophrenia patients (EOSs), brain of whom may undergo cortical network reorganization and refinement [10]. FC among these individualized networks were used as training features to predict five schizophrenic symptom domains: positive symptom, negative symptom, depression, cognition and excitement, respectively [11]. We speculated that individual-specific FC could serve as useful neuromarkers for multiple symptom domains in EOSs.

2. Methods

2.1. Participants

We recruited 39 right-handed antipsychotic-naïve EOSs with the same inclusion criteria as our previous study [12]. Five-dimensional clinical symptoms were estimated using the Positive and Negative Syndrome Scale (PANSS) (Table 1). Three EOSs were excluded for incomplete scanning, one for excessive head motion, and five due to poor image quality. Ultimately, data for 30 EOSs were used in further analysis. All patients were aged 12 to 18 years old (15 men; mean ±

SEM age, 15.10 years ± 0.32). Written informed consent of participants and approval of research ethical committee were obtained before study.

Table 1. PANSS items included in each dimension. Mean ± SEM; the 30-item PANSS including subscales for positive (P1-7 items), negative (N1-7 items), and general symptoms (G1-16 items).

Dimensions	Items	Scores
Positive	P1, P3, P5-6, N7, G1, G9, G12	22.40 ± 0.78
Negative	N1-4, N6, G7, G16	21.13 ± 1.79
Excitement	P4, P7, G8, G14	8.13 ± 0.95
Cognition	P2, N5, G5, G10-11, G13, G15	17.60 ± 0.85
Depression	G2-4, G6	4.67 ± 0.26

2.2. Data preprocessing

Resting-state functional images and T1-weighted anatomical images of participants were collected using a 3T MRI scanner (Siemens, Germany). Detail acquisition parameters have been described in our previous study [12]. Imaging data were preprocessed using the FreeSurfer and FSL packages as previously described [13].

2.3. Identifying individual-specific functional regions of interest (ROIs)

The analytical procedure has been previously described [9]. Briefly, we used the iterative parcellation algorithm to map 18 individual-level cortical networks based on a group-level functional network atlas [13]. Functional network boundaries for each individual were iteratively adjusted by using the inter-individual variability. These individualized networks were further segmented into 116 discrete ROIs. FC among homologous individual-specific ROIs was calculated for symptom prediction analysis.

2.4. Predicting specific symptom domains

Based on individual-specific FC, we used the L2-regularized and L2-loss support vector machine for regression (SVR; using the default parameter C = 1) in the Library for Support Vector Machines toolbox to predict the severity of symptoms in EOSs. Sex and head motion (mean FD) were regressed. The 10-fold cross validation (CV) approach was applied to avoid biased estimates. To reduce redundancy and prevent over-fitting, we used connections that were significantly correlated with symptoms ($P < 0.01$) as training features in each CV. The correlation between observed and predicted scores was calculated. A permutation test (5000 permutations) was performed to determine the statistical significance.

2.5. Quantifying the contributions of features

The weight score of each feature in the SVR model was calculated to quantify its contribution to symptom prediction. The weight of each feature was evaluated by summing the times that the feature is not zero across all folds. These ROI-level features were further summed and grouped into network-level connections among seven large-scale functional networks, including the visual (VIS), sensorimotor (MOT), attention (ATN), salience (SAL), frontoparietal (FPN), limbic (LMB), and default model (DMN) networks. Their network-level weights (between- or within-networks) were estimated by summing the weights of between- or within-network connections in the prediction model.

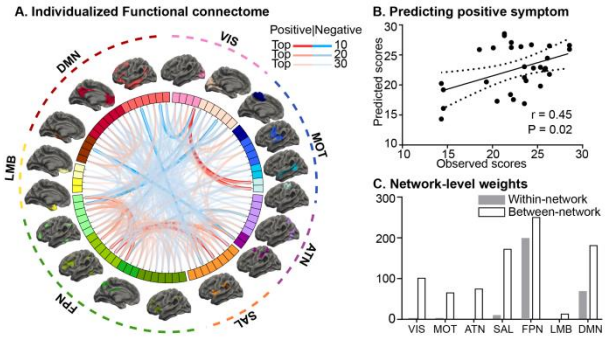


Fig.1 Individual-level positive symptom prediction model

3. Results

Eighteen individual-specific cortical functional networks were mapped and matched to 116 discrete ROIs by using an iterative parcellation algorithm. These fine-grained networks were further grouped into seven large-scale functional networks, including VIS, MOT, ATN, SAL, FPN, LMB, and DMN. FC among these individually specified ROIs were examined and used to identify neuromarkers underlying five symptom domains in EOSs. Positive scores ($r = 0.45$, $P = 0.02$; Fig.1 and depression scores ($r = 0.43$, $P = 0.03$; Fig.2 could be separately predicted by distinct sets of individualized connections, while other scores could not. Within- and between-network connections of FPN had dominated contributions to the prediction model of positive dimension (Fig.1C); and between-network connections of DMN contributed most to depression symptom prediction (Fig.2C).

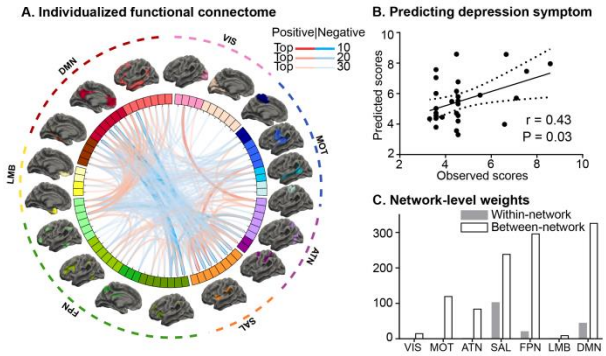


Fig.2 Individual-level depression prediction model

4. Discussions

The current study identified cortical FC among individual-specific brain areas that could yield significant predictions of multiple symptom domains in drug-naïve EOSs. Consistently, robust predictive performance has also been demonstrated for the individual strategy in other psychiatric illnesses including depression [9] and obsessive-compulsive disorder [8]. Considering greater inter-individual variability in pediatric brains than adult brains [14], aligning individuals' data to an "average brain" may obscure neuroanatomical boundaries, thereby disturbing neuroimaging results in pediatrics. The current findings highlight a feasible individual-level strategy that account for the inter-individual variability in functional region boundaries, which could be used in future research of early-onset diseases.

Positive symptom in EOSs could be tracked by FPN-based individualized FC biomarkers. Specifically, whether within-network or between-network connections of the FPN contributed largely to positive symptom prediction, which was in accord with previous findings in adult-onset schizophrenia [9]. The FPN is a high-order executive control network that could continuously update to attended stimuli for adapting to the environment [15]. Functional connections within the FPN, as well as between the FPN, DMN and SAL, were modulated by working memory load. Disrupted functional integration and segregation of the FPN were implicated to be potential causes of hallucinations and disturbed monitoring of inner speech generation in schizophrenia. Therefore, the current findings confirm the vital role of FPN in positive symptom manifestation of schizophrenia, indicating the reliability of our individual-level approach.

Depression in EOSs could be approximately predicted by connections among the DMN, FPN, SAL and MOT, where the DMN had the most contribution. Depressive syndromes, i.e., prominent subjectively low mood, are common in schizophrenia. Schizophrenia patients with depression have poorer outcomes relative to those without. Although few studies investigated the association between brain functional network abnormalities and depression in EOSs, dysconnectivity of the DMN has been consistently reported in patients with psychotic depression [16]. The current study revealed, for the first time, the neural substrates underlying depressive syndromes in EOSs. More importantly, the individual-level findings shed new insights into personalized circuit-specific therapies for depression symptom in schizophrenia or other psychotic disorders.

5. Conclusions

The novel findings reveal individual-level FC biomarkers underlying positive and depression symptoms in EOSs, which may aid in future personalized target-therapy schemes for this disorders.

Acknowledgements

This paper is supported by the National Natural Science Foundation of China (61533006, 61673089, 81471653, 81771919 and U1808204), Key Project of Research and Development of Ministry of Science and Technology (2018AAA0100705), Sichuan Science and Technology Program (2018TJPT0016).

References

[1] TREGELLAS J R. Neuroimaging biomarkers for early drug development in schizophrenia. Biological Psychiatry, Vol 76, No. 2, pp. 111-119, 2014.

[2] YAMADA T, HASHIMOTO R I, YAHATA N, et al. Resting-State Functional Connectivity-Based Biomarkers and Functional MRI-Based Neurofeedback for Psychiatric Disorders: A Challenge for Developing Theranostic Biomarkers. The International Journal of Neuropsychopharmacology, Vol 20, No. 10, pp. 769-781, 2017.

[3] VIVIANO J D, BUCHANAN R W, CALARCO N, et al. Resting-State Connectivity Biomarkers of Cognitive Performance and Social Function in Individuals With Schizophrenia Spectrum Disorder and Healthy Control Subjects. Biological Psychiatry, Vol 84, No. 9, pp. 665-674, 2018.

[4] MUELLER S, WANG D, FOX M D, et al. Individual variability in functional connectivity architecture of the human brain. Neuron, Vol 77, No. 3, pp. 586-589, 2013.

[5] GORDON E M, LAUMANN T O, ADEYEMO B, et al. Individual-specific features of brain systems identified

with resting state functional correlations. NeuroImage, 2017, Vol 146, pp. 948-939, 2017.
[6] LI M, WANG D, REN J, et al. Performing group-level functional image analyses based on homologous functional regions mapped in individuals. PLoS Biology, Vol 17, No. 3, pp. e2007032, 2019.
[7] WANG D, BUCKNER R L, FOX M D, et al. Parcellating cortical functional networks in individuals. Nature Neuroscience, Vol 18, No. 12, pp. 1853-1860, 2015.
[8] BRENNAN B P, WANG D, LI M, et al. Use of an Individual-Level Approach to Identify Cortical Connectivity Biomarkers in Obsessive-Compulsive Disorder. Biological psychiatry Cognitive Neuroscience and Neuroimaging, Vol 4, No. 1, pp. 27-38, 2019.
[9] WANG D, LI M, WANG M, et al. Individual-specific functional connectivity markers track dimensional and categorical features of psychotic illness. Molecular Psychiatry, 2018.
[10] GOGTAY N, GIEDD J N, LUSK L, et al. Dynamic mapping of human cortical development during childhood through early adulthood. Proceedings of the National Academy of Sciences of the United States of America, Vol 101, No. 21, pp. 8174-8179, 2004.
[11] MARDER S R, DAVIS J M, CHOUINARD G. The effects of risperidone on the five dimensions of schizophrenia derived by factor analysis: Combined results of the North American trials. The Journal of Clinical Psychiatry, Vol 58, No. 12, pp. 538-546, 1997.
[12] LI M, BECKER B, ZHENG J, et al. Dysregulated Maturation of the Functional Connectome in Antipsychotic-Naive, First-Episode Patients With Adolescent-Onset Schizophrenia. Schizophrenia Bulletin, Vol 45, No. 3, pp. 689-697, 2019.
[13] YEO B T, KRIENEN F M, SEPULCRE J, et al. The organization of the human cerebral cortex estimated by intrinsic functional connectivity. Journal of Neurophysiology, Vol 106, No. 3, pp. 1125-1165, 2011.
[14] FOULKES L, BLAKEMORE S J. Studying individual differences in human adolescent brain development. Nature Neuroscience, Vol 21, No. 3, pp. 315-323, 2018.
[15] DUNCAN J. The multiple-demand (MD) system of the primate brain: mental programs for intelligent behaviour. Trends in Cognitive Sciences, Vol 14, No. 4, pp. 172-179, 2010.
[16] SCHILBACH L, HOFFSTAEDTER F, MÜLLER V, et al. Transdiagnostic commonalities and differences in resting state functional connectivity of the default mode network in schizophrenia and major depression. Neuroimage-Clinical, Vol 10, pp. 326-335, 2016.

ALTERED INTER-HEMISPHERIC FUNCTIONAL CONNECTIVITY DYNAMICS IN BIPOLAR DISORDER

YANG YANG[1], CUI QIAN[2*], CHEN HUAFU[1*]

[1]School of Life Science and Technology, University of Electronic Science and Technology of China
[2]School of Public Affairs and Administration, University of Electronic Science and Technology of China
E-MAIL: 991826390@qq.com, *chenhf@uestc.edu.cn, *qiancui26@gmail.com

Abstract:

Inter-hemispheric connectivity (IHC) take part in emotional, cognitive, and sensorimotor information integration. Nevertheless, all these identified IHC changes in bipolar disorder (BD) were based on the assumption that IHC are static. We incorporated sliding-window method into IHC to investigate the temporal variability of IHC in 40 BD patients and 60 healthy controls (HCs). We found patients group showed increased dynamic IHC in the cerebellum, inferior frontal gyrus of orbit, temporal, and sensorimotor network. While reduced dynamic in the posterior parietal and precuneus. In addition, we found the correlation between No. of depressive episodes and altered dynamic VMHC in Postcentral Gyrus in BD group. Our finding provide a new perspective about the pathomechanism of BD.

Keywords:

Bipolar disorder; Depression; interhemispheric; Dynamic functional connectivity

1. Introduction

Bipolar disorder (BD) patients have fluctuating episodes of depression and hypomania or mania. Depressive episodes are three times more than other mood episodes in BD and exacerbate patients' quality of social life. Except for emotion damage, BD patients also suffering cognition deficits. The evidence for the pathophysiological mechanism is lacking [1]. With the progress of functional magnetic resonance imaging (fMRI) and information science, we can see more brain function by using these tools.

Although situated at the brain with a large anatomic distance, functional connectivity (FC) of hemisphere homologous regions was higher than others [2]. This was attributed to the fundamental role of corpus callosum (CC), the biggest fiber bundles connected between two hemisphere, in coordinating emotional, cognitive, and sensorimotor information integration [3]. Previous diffusion tensor imaging study revealed significantly lower structural integrity in the anterior section of the CC in BD patients compared with healthy individuals, independent of the patients' affective state [4]. Due to these abnormal CC structure in BD, interhemispheric functional dysconnectivity was found [5]. Another study demonstrated disrupted interhemispheric FC between the default mode network (DMN) regions in BD during major depressive episodes (BDD) [6].

Nevertheless, all these identified interhemispheric connectivity (IHC) changes in BD were based on the assumption that IHC are static. Recent advances in resting-state FC demonstrated that brain regions exhibits physiologically significant time-varying interflow [7]. Also, previous study defined interhemispheric functional modules in a task state, and concluded that they work through dynamic communication [8]. A recent study found the associations between dynamic functional interhemispheric connectivity and cognitive processes [9].

Voxel mirrored homotopic connectivity (VMHC) is a common method to calculate IHC of every pair of hemispheric mirrored voxel. Sliding-window (SW) method is a frequently-used dynamic FC analysis tool. In the current study, we incorporated SW analysis into VMHC analysis to investigate the temporal variability of the IHC in BDD and healthy controls.

2. Methods

A total of 40 BDD patients and 60 healthy controls (HCs) were included in this study. Written informed consent of each participant and the study approval report by the research ethical committee were described in our previous paper [10].

2.1. MRI data acquisition

A 3 tesla General Electric MR750 scanner located in the UESTC was used to collect the MRI data of all participants. The parameter of MRI data acquisition were reported in our previous paper [10].

2.2. Preprocessing

We preprocessed the MRI data with a neuroimaging toolbox, namely, DPABI. For individual functional images, due to subjects need to adapt to the magnetic resonance environment, the first five images were discarded. Then, we did slice-timing and realign. The maximum displacement and angular motion were no more than 3 mm and 3°, respectively. Several spurious covariates were regressed. The individual structural images were coregistered to their functional images and were then segmented and normalized into standard space using the DARTEL algorithm. Applied the parameters of structural image normalization to functional images. Then these images were Gaussian kernel smoothed with FWHM equal to 6 mm. Subsequently, linear trend was removed and then were filtered to 0.01–0.08 Hz. Finally, the individual images were registered to a hemispheric symmetrical structural template [11].

2.3. Dynamic VMHC analysis

Dynamic VMHC was calculated using SW analysis with DPABI. First, we applied hamming windows with length =30 TRs and overlap = 1 TR to preprocessed signals, according to the criteria that window length should be choosed within 15 TRs to 30 TRs [12]. Then we calculated VMHC as the FC between every pair of mirrored voxel signal within each window for each participant. Finally, we used the coefficient of variation (CV) that was computed as std/mean of VMHC map across time windows. Before statistical analysis, the CV maps were Z-standardized.

2.4. Statistical analysis

Two sample t statistic was used to observe group differences in CV images. AlphaSim method that combine of voxel 0.01 and two-tailed cluster 0.05 was used to fulfill a multiple comparison. Individual's demographic information were used as spurious covariates. Finally, we did correlative analysis between CV values of significant different regions and clinical scales.

3. Results

Demographic and clinical information were shown in Table1.

3.1. Group changes in CV

The BDD group showed higher CV than HCs in Cerebelum_6,Cerebelum_8,Frontal_Inf_Orb,Temporal_Sup, Postcentral Gyrus (PG), and Supp_Motor_Area (Fig. 1, Table 2). While, the patient group showed reduced CV in the Superior Parietal Lobule, Angular Gyrus, and Precuneus than the control group (Fig. 2, Table 2). There was significant correlations between the No. of depressive episodes and altered CV in PG in BDD patients (Fig. 3).

Table 1 Demographic information.

Variables	HC	BDD	P
Age	31±10.18	34.43±10.76	0.11
Sex(M/F)	32/28	22/18	0.87
Handedness(L/R)	1/59	1/39	0.77
Education	14.32±3.93	13.70±3.04	0.40
Head motion	0.09±0.04	0.10±0.07	0.54
Age of first onset	-	27.03±9.57	-
No. of depressive episode	-	2.63±1.13	-
No. of manic episode	-	1.65±1.08	-
HAMD score	-	22.93±6.41	-

Table 2 CV differences between two groups.

Brain Regions	MNI x,y,z	Cluster Size	T Value
Cerebelum_6	21,-60,-24	14	3.54
Cerebelum_8	9,-72,-39	6	2.86
Inferior Frontal Gyrus	24,27,-21	10	2,97
Superior Temporal Gyrus	57,-30,3	6	3.70
Postcentral Gyrus	54,-6,27	10	2.68
Superior Parietal Lobule	30,-69,45	6	-3.11
Angular Gyrus	36,-63,45	7	-2.60
Supp_Motor_Area	6,-12,54	6	2.83
Precuneus	15,-48,69	14	-2.90

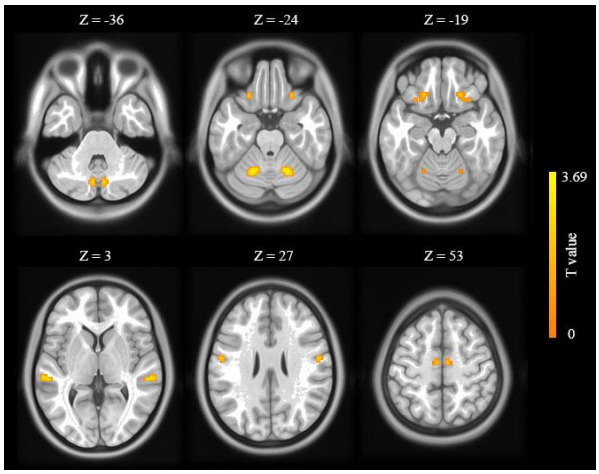


Fig.1 Higher CV of VMHC in BDD group as compared with HCs group

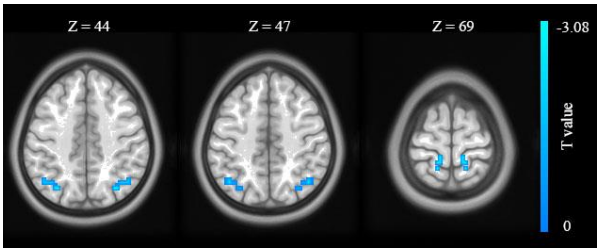


Fig.2 Reduced CV of VMHC in BDD group as compared with HCs group

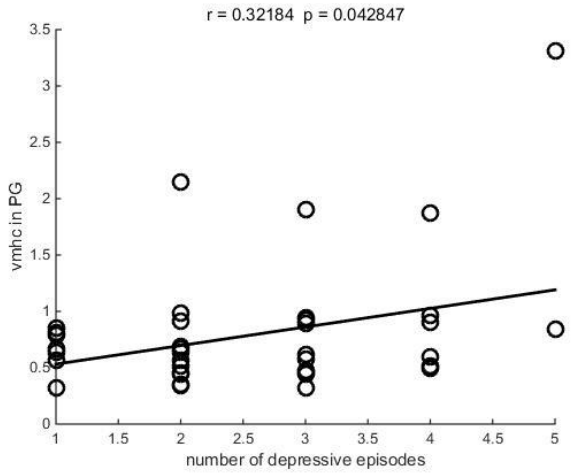


Fig.3 Correlation between the No. of depressive episodes and altered CV of VMHC in Postcentral Gyrus in BDD patients

4. Discussion

We investigated the dynamic interhemispheric connectivity alterations in BDD patients using SW analysis. Results revealed significantly increased dynamic in the external-oriented system in the BDD when compared to HCs group. The higher dynamic in PG was correlated with the No. of depressive episodes in BDD patients. In addition, reduced dynamic in the internal-oriented system was also found. Overall, these findings suggested the abnormal dynamic interhemispheric connectivity underlying the pathological mechanisms of BDD.

4.1 Unstable interhemispheric connectivity

We found increased dynamic interhemispheric connectivity in cerebelum, sensorimotor network (SMN), and temporal cortex in patients with BDD. Except for control and motor coordinate, recently, more and more findings suggested cerebellum play an important role in perception and cognitive function. A dynamic reating state study found BDD spent more time in a network FC state associated with cerebellum. Structural abnormalities of cerebellum have also been reported in BDD. BDD patients often have psychomotor agitation and behavioral inhibition. Unstable connectivity in the SMN may imply psychomotor symptoms in BDD. Also, somatosensory related areas are associated with response to emotional facial expressions. Higher dynamic in PG correlated with the No. of depressive episodes implied that SMN might associated with depression in BDD patients. Some previous study concluded that cognitive and emotional related temporal cortex circuits is associated with the pathological mechanisms of BDD. Previous study showed significantly increased connectivity between left amygdala and orbitofrontal cortex (OFC) in BDD. Our finding of unstable interhemispheric connectivity provide a new evidence for BDD could be conceptualized as parallel decreased FC in bilaterally OFC-amygdala emotion circuits.

4.2 Hyperstable interhemispheric connectivity

BDD patients showed hyperstable IHC in the DMN regions. A recent research found increased within-network while decreased inter-network FC in DMN in BD. Another study found aberrant whole-brain FC of DMN regions in BDD [13]. Moreover, the DMN and SMN showed disbalance in interhemispheric connectivity dynamic that may be related to cognitive symptoms in BDD [14].

5. Conclusions

Through the sliding time-window analysis, we investigated the dynamic interhemispheric connectivity alterations in the BDD patients. Unstable interhemispheric connectivity in ventral frontal, temporal, cerebelum, and sensorimotor network might be associated with sensory and psychomotor symptoms, emotion processing and regulation deficts. Hyprestable interhemispheric connectivity in the DMN regions might be imply the cognitive symptoms in the BDD patients. In addition, the correlation between higher dynamic in postcentral gyrus and disease progression that worth to be explored in the future.

Acknowledgements

We thank some funding sources. The Key Project of Research and Development of Ministry of Science and Technology (2018AAA0100705), the Natural Science Foundation of China (62036003, U1808204, 81771919).

References

[1] Conio, B., et al., Opposite effects of dopamine and serotonin on resting-state networks: review and implications for psychiatric disorders. Molecular Psychiatry, 2020. 25(1): p. 82-93.

[2] Salvador, R., et al., Neurophysiological Architecture of Functional Magnetic Resonance Images of Human Brain. Cerebral Cortex, 2005. 15(9): p. 1332-1342.

[3] Fan, H., et al., Analysis of voxel-mirrored homotopic connectivity in medication-free, current major depressive disorder. Journal of Affective Disorders, 2018. 240: p. 171-176.

[4] Matsuoka, K., et al., Microstructural Differences in the Corpus Callosum in Patients With Bipolar Disorder and Major Depressive Disorder. 2017. 78(1).

[5] Yasuno, F., et al., Interhemispheric functional disconnection because of abnormal corpus callosum integrity in bipolar disorder type II. 2016. 2(6): p. 335-340.

[6] Wang, Y., et al., Reduced interhemispheric resting‐state functional connectivity in unmedicated bipolar II disorder. 2015. 132(5): p. 400-407.

[7] Allen, E.A., et al., Tracking Whole-Brain Connectivity Dynamics in the Resting State. 2014(3): p. 663-676.

[8] Doron, K.W., D.S. Bassett, and M.S.J.P.N.A.U.S.A. Gazzaniga, Dynamic network structure of interhemispheric coordination. 2012. 109(46): p. 18661-18668.

[9] Lin, S.J., et al., Both Stationary and Dynamic Functional Interhemispheric Connectivity Are Strongly Associated With Performance on Cognitive Tests in Multiple Sclerosis. 2020. 11.

[10] Yang, Y., et al., Frequency-specific alteration of functional connectivity density in bipolar disorder depression. 2020. 104: p. 110026.

[11] Zuo, X.-N., et al., Growing Together and Growing Apart: Regional and Sex Differences in the Lifespan Developmental Trajectories of Functional Homotopy. The Journal of Neuroscience, 2010. 30(45): p. 15034.

[12] Zalesky, A. and M. Breakspear, Towards a statistical test for functional connectivity dynamics. NeuroImage, 2015. 114: p. 466-470.

[13] Wang, Y., et al., Disrupted Resting-State Functional Connectivity in Nonmedicated Bipolar Disorder. 2016: p. 529.

[14] Martino, M., et al., Contrasting variability patterns in the default mode and sensorimotor networks balance in bipolar depression and mania. Proceedings of the National Academy of Sciences, 2016. 113(17): p. 4824.

GAN-BASED SYNTHETIC GASTROINTESTINAL IMAGE GENERATION

PRINCE. E. ADJEI[1,2,3], ZENEBE M. LONSEKO[1,2], NINI RAO[1,2]

[1]Key Laboratory for Neuro-information of Ministry of Education, University of Electronic Science and Technology of China, Chengdu, China
[2]School of Life Science and Technology, University of Electronic Science and Technology of China, Chengdu, China
[3]Department of Computer Engineering, Kwame Nkrumah University of Science and Technology, Ghana
E-MAIL: raonn@uestc.edu.cn

Abstract:

As with several medical image analysis tasks based on deep learning, gastrointestinal image analysis is plagued with data scarcity, privacy concerns and insufficient number of pathology samples. This paper frames the task of generating new and plausible samples of oesophageal cancer images as an image-to-image translation task. We evaluate two adversarial trained fully convolutional network architectures to generate synthetic diseased gastrointestinal images from segmentation maps prepared by expert clinicians. The synthetic images are evaluated both qualitatively and quantitively and the experimental results indicate that they are comparable to the original images. This potentially addresses the challenge of data scarcity and the need for heavy data augmentation in automated gastrointestinal image analysis.

Keywords:

Generative Adversarial Networks; Gastrointestinal Imaging; Pix2Pix

1. Introduction

An automated approach to the analysis of gastrointestinal images offers objective and reliable measurements on a large scale that have the potential to improve on medical decision making; something that would be manually impossible to achieve. Several researchers have proposed different techniques for automated analyses of gastrointestinal images including detection of lesions [1]. A detailed review of the utilization of deep learning in this field is presented in [2]. Deep learning techniques however require large amounts of data for high performance especially on a diverse data set like esophageal cancer images. Obtaining gastrointestinal samples can be challenging. First of all, patient consent could be mandatory especially where the data is intended to be released or used in public. Secondly, labeling gastrointestinal images is labor intensive and time-consuming. Finally, there is insufficient number of positive cases for each pathology. Traditionally, the approach to remedy the challenge of insufficient samples is to geometrically transform existing samples and re-sample the transformed images as new samples in order to create a diverse data set (known as data augmentation). This approach however has limitations in gastrointestinal imaging and medical imaging in general. A potential solution is to generate entirely new but plausible samples either diseased or normal; ensuring that the issue of privacy is addressed since the generated images are synthetic. Again, generative models can be designed to identify anomalies [3] thereby augmenting the work of clinicians and reducing the need for annotation. Since originally proposed in [4], generative adversarial networks (GANs) have shown great potential in several applications in medical imaging. Current applications of GANs in medical image generation are however mostly limited to low resolution radiology images [5] (which can be considered as gray scale images), and recently in ophthalmology [6]. The goal of this paper is to demonstrate the applicability of the pix2pix framework [7] for generating high quality esophageal cancer images for subsequent downstream applications.

2. Network Architecture

The GAN is a framework for training a generative model in an adversarial manner. Two neural networks are at the heart of the vanilla GAN; a generator *G* and discriminator *D* that participate in a zero-sum game. *G* takes random noise as input and outputs fake data samples aiming to maximize the probability of deceiving *D* whiles *D* acts a binary classifier with the objective of deciphering real training samples from generated samples produced by the generator. *D* minimizes the cross-entropy loss between original and generated data samples in order to achieve its goal. In the vanilla GAN convergence is accomplished by achieving a Nash balance [4].

2.1. Pix2Pix Architecture

The pix2pix architecture is an implementation of cGAN [8] and a generic solution to image-to-image translation. In an image-to-image translation task, the input to *G* is conditioned on an image (source image) with the goal of translating it into a target image. *D* takes the source image and the target image and must determine whether the source is reasonably converted into the target image. Fundamentally, both the *G* and the *D* consist of Convolution-batch normalization-ReLU blocks. *G* is designed as a U-Net model [9] with skip connections between corresponding layers in the encoder and the decoder. This design ensures the transfer of low-level details from source image to target image. *D* is designed to classify the input image's 70x70 patch size as either real or fake and is implemented as a deep convolutional network. The overall output of *D* is an average of all activations across the input image. In medical image analysis, the pix2pix architecture was applied for example in [10] where the authors modified the generator architecture for PET-CT translation, correcting MR motion artefacts and denoising PET images. In [11], the authors added a gradient-based loss function to a pix2pix loss function for the generation of CT images from source MRI and 7T MRI from source 3T MRI. In [12], a pix2pix based GAN was developed with Wasserstein loss and perceptual loss to denoise CT scans. In this work we aim to generate new and plausible samples of gastrointestinal colour images using a pix2pix based architecture.

3. Materials and Methods

3.1. Data

A total of 260 esophageal cancer images were used for this study. The data for the experiment was obtained from Digestive Endoscopy Center, West China Hospital, Sichuan University. For each image, gastroenterologists marked out diseased locations on the image and from the markings, binary images (segmentation maps) were produced (Figure 4.i). The images are each of size 512x512.

3.2. Experimental Setup

Figure 1 shows an overview of the experimental setup. Aiming at the generation of entirely new and plausible samples of esophageal cancer images, we framed this problem as an image-to-image translation task; using segmentation maps for esophageal cancer diseases as source images for generation of new and plausible samples of target esophageal cancer images. Each segmentation map input, denoted $X \in \mathbb{R}^{HxW}$, where H represents height and W represents the width of the binary image is paired with a corresponding colour cancer image denoted $Y \in \mathbb{R}^{HxWx3}$ and fed as input into *G*. *X* is resized from 512x512 to 256x256 to decrease computational load. We use a batch size of 1.

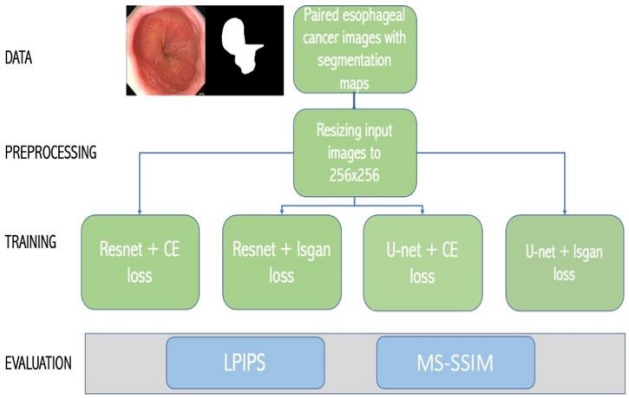
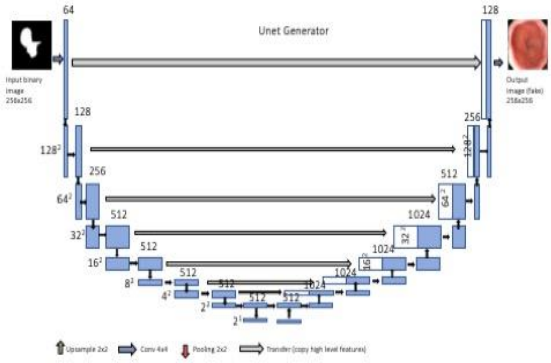


Fig.1 Overview of Experimental Setup

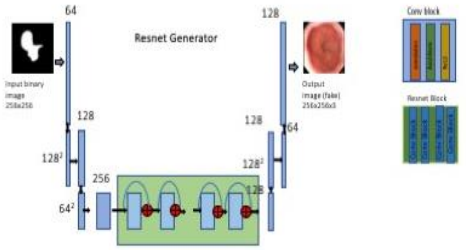
3.3. Architecture

3.3.1. Generator Architecture

Two variants of *G* are implemented in this work for generation task. The architectures are based on the U-Net [9] with improvements to avoid the typical bottleneck in the traditional encoder-decoder network architecture. *G* adds skip connections between corresponding encoder-decoder layers, as shown in figure 2a. As concatenations of all channels at layer *i* with those at layer *n-i*, skip connections are added, where *n* is the total number of layers [7]. The Resnet architecture replaces the bottleneck with residual units and skip connections as shown in figure 2b, following the concept by [13]. *G* does not draw samples from a latent vector *Z*, rather randomness is achieved by using drop out layers in the last three layers of the decoder during both training and prediction; so-called instance normalization [14].



a



b

Fig.2 a. U-net generator architecture b. Resnet generator Architecture

3.3.2. Discriminator Architecture

An overview of the PatchGAN discriminator implemented in this work is presented in Figure 3. The discriminator consists of four convolution blocks to map the input to a 1-dimensional output followed by a 1x1 convolution layer whose output is fed into a sigmoid function for a prediction score of how real or fake the input image is. The architecture is summarized as C64-C128-C256-C512-ouput, where each *C* layer consists of Convolution, batch normalization and ReLu activation apart from the C64 layer which excludes a batch normalization layer. This architecture classifies a 70x70 patch of the input image as either fake or real. The final feature map is an average of each 70x70 patch area in the 256x256 input image. *G* learns faster than *D*, and so the rate of learning for *D* is slowed by 0.5.

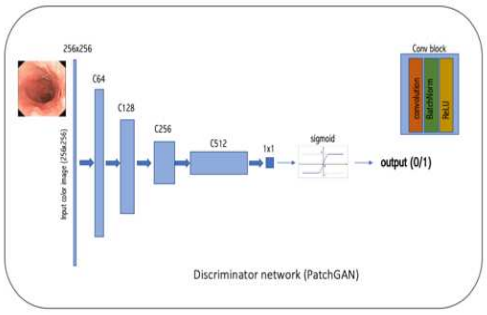


Fig.3 PatchGAN discriminator

3.4. Loss Functions

The vanilla GAN *G* learns a mapping to an output image *Y* from a random noise vector *Z; G: Z → Y.* On the other hand, cGAN learns to map the observed image *X* and random vector *Z* to *Y; G: {X, Z} → Y.* The task will adapt the minmax training strategy (1) whose objective function is given by (2), (3) and (4).

$$min_G max_D V^*(G, D) \quad (1)$$

$$V^*(G, D) = L^{(G)}(\theta_G, \theta_D) + L^{(D)}(\theta_G, \theta_D) \quad (2)$$

$$L^{(D)} = \mathbb{E}_{X,Y} \log(D(X, Y)) + \mathbb{E}_{X,Z} \log(1 - D(G(X, Z))) \quad (3)$$

$$L^{(G)} = -\mathbb{E}_{X,Z}[\log(D(X, G(X, Z))] + \lambda \mathbb{E}_{X,Y,Z}[||Y - G(X, Y)||_1] \quad (4)$$

where L^D is the loss for *D* and L^G is the loss for *G*. We train the models using cross-entropy loss and the least squares loss (LSGAN) [15]. Lambda (λ) controls the contribution of the regression loss to the composite loss function of the generator, influencing *G* to produce images that are a plausible translation of the source image. λ is set to 100.

3.5. Evaluation metrics

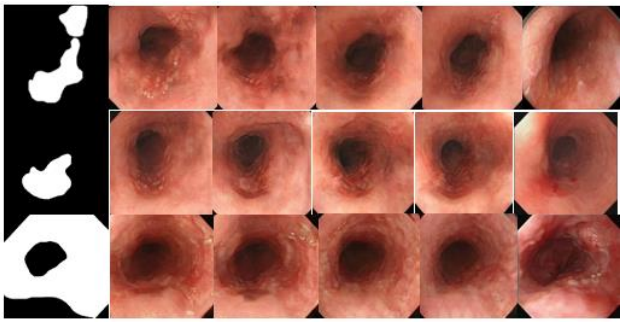
There is still no consensus on the most ideal metrics to assess generative models [16] and so it remains an active area of research. To evaluate the images produced in this work, we employ traditional quantitative measurement technique; Multiscale Structural Similarity Index (MS-SSIM) [17] and recently proposed perceptual image path similarity score (LPIPS) [18]. LPIPS closely matches the response of human evaluation of images produced by GANs and has been employed in a similar task by [10] to evaluate radiology images produced by GAN.

4. Results

4.1 Qualitive Analysis

Figure 4 shows the results of the two architectures with different loss functions for the task of synthesizing new and plausible esophageal cancer images from segmentation maps. From the figure, the U-Net achieves better human visual perception compared to the Resnet architecture. The diseased portions inferred from the segmentation maps appear exaggerated in the Resnet architecture. The LSGAN loss functions also appear to generally produce less bright and blur images. The U-Net architecture produces plausible diseased images without exaggerating the colour of the lesions. Quantitatively assessing the performance of both architectures and loss functions corroborates human perception.

4.2 Quantitative Evaluation



i ii iii iv v vi

Fig.4 (i) input segmented map (ii) Resnet + CE loss (iii) Resnet + LS loss (iv) U-net + CE loss (v) U-net + LS loss (vi) Ground truth

Table 1

Resnet	**Cross-entropy**	**LSGAN**
MS-SSIM	0.9987	0.9987
LPIPS	0.4956	0.5001
U-net		
MS-SSIM	*0.9989*	0.9986
LPIPS	*0.4872*	0.4921

Table 2 summarizes the performance of both architectures. It can be observed that the U-Net with cross-entropy loss demonstrates better performance compared to the Resnet architecture in terms of MS-SSIM and LPIPS, which corroborates qualitative evaluation. The LSGAN loss function even though more stable during training does not produce images of high quality.

5. Conclusion

In this work, we propose the concept of framing the generation of entirely new and plausible samples of medical images to augment scarce samples as an image-to-image translation task. Using segmentation maps generated from gastrointestinal images, we use the supervised pix2pix framework to generate new samples. We evaluate the concept using two architectures; Resnet and U-Net based, and also on two loss functions; the vanilla cross-entropy loss and the LSGAN. The synthetic images are plausible and may be useful for other downstream tasks including segmentation and detection. The results demonstrate that GANs can be useful for generating new and plausible samples of medical images to compliment the traditional data augmentation techniques for dealing with scarce samples. Future work will explore new techniques for improving on image quality and investigate the relationship between synthetic images and the performance of computer-aided diagnosis systems.

Acknowledgements

This paper is supported in part by the National Natural Science Foundation of China under Grant 61872405 and Grant 61720106004, and in part by the Key R&D Project of Sichuan Province (2020YFS0243).

References

[1] D. Y. Liu *et al.*, "Identification of lesion images from gastrointestinal endoscope based on feature extraction of combinational methods with and without learning process," *Med. Image Anal.*, vol. 32, pp. 281–294, 2016.

[2] W. Du *et al.*, "Review on the Applications of Deep Learning in the Analysis of Gastrointestinal Endoscopy Images," *IEEE Access*, vol. 7, pp. 142053–142069, 2019.

[3] T. Schlegl, P. Seeböck, S. M. Waldstein, G. Langs, and U. Schmidt-Erfurth, "f-AnoGAN: Fast unsupervised anomaly detection with generative adversarial networks," *Med. Image Anal.*, vol. 54, pp. 30–44, 2019.

[4] I. J. Goodfellow *et al.*, "Generative adversarial nets," *Adv. Neural Inf. Process. Syst.*, vol. 3, no. January, pp. 2672–2680, 2014.

[5] X. Yi, E. Walia, and P. Babyn, "Generative adversarial network in medical imaging: A review," *Med. Image Anal.*, vol. 58, p. 101552, 2019.

[6] Z. Yu, Q. Xiang, J. Meng, C. Kou, Q. Ren, and Y. Lu, "Retinal image synthesis from multiple-landmarks input with generative adversarial networks," *Biomed. Eng. Online*, vol. 18, no. 1, pp. 1–15, 2019.

[7] P. Isola, J. Y. Zhu, T. Zhou, and A. A. Efros, “Image-to-image translation with conditional adversarial networks,” *Proc. - 30th IEEE Conf. Comput. Vis. Pattern Recognition, CVPR 2017*, vol. 2017-Janua, pp. 5967–5976, 2017.
[8] M. Mirza and S. Osindero, “Conditional Generative Adversarial Nets,” pp. 1–7, 2014.
[9] O. Ronneberger, P. Fischer, and T. Brox, “U-net: Convolutional networks for biomedical image segmentation,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9351, pp. 234–241, 2015.
[10] K. Armanious *et al.*, “MedGAN: Medical image translation using GANs,” *Comput. Med. Imaging Graph.*, vol. 79, 2020.
[11] D. Nie *et al.*, “Medical Image Synthesis With Deep Convolutional Adversarial Networks,” *IEEE Trans. Biomed. Eng.*, vol. 67, no. 9, p. 2706, 2020.
[12] Q. Yang *et al.*, “Low-Dose CT Image Denoising Using a Generative Adversarial Network With Wasserstein Distance and Perceptual Loss,” *IEEE Trans. Med. Imaging*, vol. 37, no. 6, pp. 1348–1357, 2018.
[13] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, vol. 2016-Decem, pp. 770–778, 2016.
[14] D. Ulyanov, A. Vedaldi, and V. Lempitsky, “Instance Normalization: The Missing Ingredient for Fast Stylization,” no. 2016, 2016.
[15] X. Mao, Q. Li, H. Xie, R. Y. K. Lau, Z. Wang, and S. P. Smolley, “Least Squares Generative Adversarial Networks,” *Proc. IEEE Int. Conf. Comput. Vis.*, vol. 2017-Octob, pp. 2813–2821, 2017.
[16] A. Borji, “Pros and cons of GAN evaluation measures,” *Comput. Vis. Image Underst.*, vol. 179, pp. 41–65, 2019.
[17] Z. Wang, E. Simoncelli, and A. C. Bovik, “Mssim,” *New York*, vol. 2, pp. 9–13, 2003.
[18] R. Zhang, P. Isola, A. A. Efros, E. Shechtman, and O. Wang, “The Unreasonable Effectiveness of Deep Features as a Perceptual Metric,” *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, no. 1, pp. 586–595, 2018.

APPLICATION OF GENERATIVE ADVERSARIAL NETWORK IN SEMANTIC SEGMENTATION

LIU KEXIN[1], GUO CHENJUN[2]

[1]School of Glasgow, University of Electronic Science and Technology of China, Chengdu611731, China；
[2]Research Institute of Electronic Science and Technology, University of Electronic Science and Technology of China, Chengdu611731, China
E-MAIL:1932129119@qq.com, johnsonguo@uestc.edu.cn

Abstract:

In order to improve the accuracy of image segmentation without changing the structure of original semantic segmentation models, an approach to train semantic segmentation models by using generative adversarial network (SS-GAN) is proposed. Using adversarial network to distinguish the source of segmented images, the model can learn the high-order relationship between pixels to enhance the spatial continuity of pixels in the segmented image. There are three aspects related to the work: constructing the generative model of fully convolutional network (FCN) structure by using VGG, and segment image preliminarily; constructing the adversarial model and training it by combining the original images, fake segmented images and real segmented images; modifying the loss function, adding the anti-loss to assist segmentation model training, encouraging generative network to learn the inter-pixel relationship independently. Experiments on PASCAL VOC and Cityscapes datasets show that the proposed method achieves better performance than the existing advanced methods, and improves IoU by 1.56% and 1.93%, respectively.

Keywords:

Semantic segmentation; Generative adversarial network; Fully convolutional network; Spatial contiguity

1. Introduction

The most advanced semantic segmentation technologies today are implemented by convolutional neural networks (CNN). In 2014, Long et al. [1] modified the structure of high-precision classification neural networks such as AlexNet[2], GoogleNet[3], VGG[4], and proposed FCN, which realized end-to-end image semantic segmentation. And a large accuracy improvement has been achieved on multiple data sets such as PASCAL VOC，NYUDv2[5]，SIFT Flow, etc. Since then, a large number of semantic segmentation networks based on FCN structure design have appeared, such as a series of DeepLab proposed by Chen et al. [6] in 2016, which further improved the accuracy of semantic segmentation by introducing Conditional Markov Random Field and hole convolutions into the network. In 2015, U-Net [7], proposed by Ronneberger et al. designed an encoder-decoder structure based on the FCN structure for semantic segmentation. However, whether it is the segmentation model of the FCN structure or U-Net, when the pixel label is predicted in the model training, the result of each pixel is independent of other pixels. But in fact, the values of pixels that are close to each other have a certain correlation. Although various post-processing techniques are usually used to modify the segmented images to enhance their spatial continuity，they are difficult to implement and run at a slower speed.

Compared with the above methods, using GAN to assist semantic segmentation does not need to increase the amount of model parameters or modify the model structure, only through the adversarial network to explore the high-order relationship between pixels in the current image, and then enhance the spatial continuity of pixel segmentation. It is more suitable for current main semantic segmentation models to improve the segmentation accuracy.

In this paper, we try to use the GAN proposed by Goodfellow et al. [8] to mine high-order connections between pixels. The using of GAN can assist the generation model to learn high-order connections between pixels without changing the original segmentation network structure, parameter, and calculation amount.

2. SS-GAN model

This section will introduce the principle of SS-GAN model. It includes four aspects: SS-GAN model structure design, generative network model, adversarial network model, and the loss function define.

2.1. SS-GAN structure design

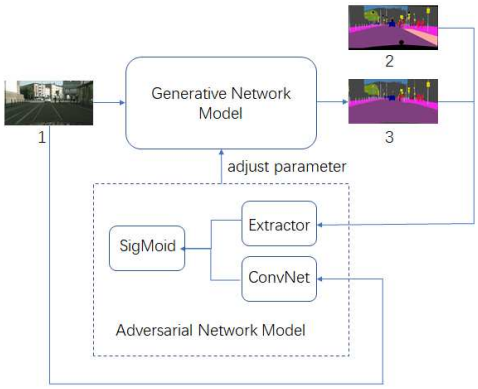


Fig.1 SS-GAN network structure

The training images are sent to the generative network (referred to as G). G extracts the semantic information and features from the input images, and generates the corresponding segmentation results. Then, the labeled segmentation results and segmentation results generated by G are sent to Adversarial Network (referred to as AN).

AN includes Extractor and ConvNet. Extractor further extracts features from the segmentation results to form a high- order feature vector. The original image is sent to ConvNet for rough extraction to supplement the original image information lost after being extracted twice by the extractor of G and AN. Then the high-order feature vectors generated by segmentation results are connected with the vectors generated by ConvNet. Finally, the sigmoid layer is used to determine whether the segmentation result input to AN belongs to the segmentation result generated by G or the segmentation result of original annotation.

According to the output of AN, the weight of G is adjusted. The purpose of this stage is to make a completely unable to distinguish whether the segmentation result currently input into AN is the result generated by G or the original annotation, to improve the segmentation effect generated by G.

2.2. Generative network model

VGG16 is chosen as the basic model of the generative network model (in Figure 1). The structural design of the VGG network is simple and regular, and easy to adjust. It has achieved excellent results in classification and detection. In the 2014 ILSVRC competition, VGG achieved a 92.3% correct rate in the Top-5.

The traditional VGG16 model is an image classification model, and after module 4 is a three-layer fully connected layer. Before entering the fully connected layer, the feature map will undergo a dimensional transformation to connect the feature vectors of the y-axis together, so that the feature map becomes a spatial vector. It is beneficial to extract semantic features，but it greatly destroys the spatial structure characteristics of the object， and semantic segmentation requires not only semantic features but also spatial characteristics of the object.

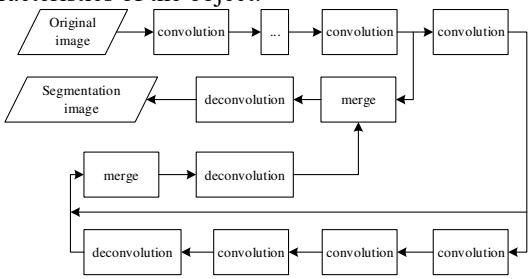


Fig.2 G-Vgg16 structure

Therefore, we use the G-VGG16 showed as Figure 2. In order to maintain the spatial characteristics of the feature map, the fully connected network is transformed into a fully convolutional layer. The weight of the fully connected layer can be transformed into the convolution kernel parameters of the corresponding fully convolutional layer through deformation. For example, for the fully convolutional layer of module 5, the weight shape corresponding to the previous fully connected layer is (25088, 4096). Since the shape of the feature vector input by the fully connected layer is (25088,), it is deformed from the feature map with shape (7,7,512), the convolution kernel size of the fully convolutional layer can be set to (7, 7), the input channel can be set to 512, and the output channel can be set to 4096. Then, transform the weights of the fully connected layer and then reusing them. Moreover, the feature map received by the first layer of deconvolution is 32 times smaller than the original image. If the feature map is directly used for deconvolution to enlarge the original image, the segmentation effect will be poor.

Table 1 The generative model structure table

Module	G-VGG16	
	Type	Parameter
0	Convolution pooling	$[3\times3,64]\times2$
1	Convolution pooling	$[3\times3,128]\times2$
2	Convolution pooling	$[3\times3,256]\times3$
3	Convolution pooling	$[3\times3,512]\times3$
4	Convolution pooling	$[3\times3,512]\times3$
5	convolution	$[7\times7,4096]\times1$
6	convolution	$[1\times1,4096]\times1$
7	convolution	$[1\times1,classes]\times1$

Therefore, after being enlarged by deconvolution, the feature map merged with the feature map output by the fourth

block into a new feature map. And so on, the new feature map, obtained after merge with the feature map output by the third block, can be interpolated and enlarged by 8 times to obtain a more refined segmentation effect. Table 1 shows the detailed network structure of G-VGG16.

2.3. Adversarial network model

In the adversarial model, unlike the general adversarial model that only inputs the generated results and the real results, the original images are also input into the model, and the features are extracted by the feature extractor and then merged with the features of the segmentation image. The network structure is shown in Figure 3.

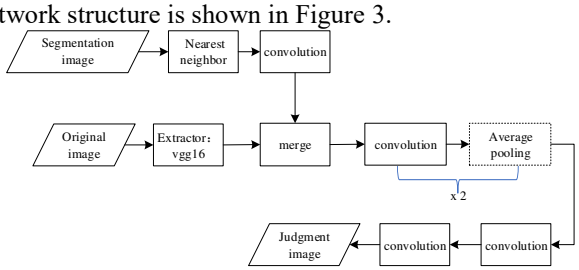


Fig.3 Structure of the adversarial model

Since the adversarial model needs to judge the source of the segmentation image, and the segmentation image itself has a simple spatial structure and highly generalized semantic information, if you directly enter the true and false segmentation image for adversarial training, it is easy to cause the adversarial model to quickly converge through the distinction of details, instead of learning the high-order relationship between pixels as expected. For example, for the real segmentation image of the input model, one-hot transformation will be performed first to turn it into a $H \times W \times classes$ feature image. For each pixel, the feature vector describing it is only 1 in the dimension of the category the pixel belongs to, and the rest are 0. The generated segmentation image passed by the generation model is also a $H \times W \times classes$ feature image, and all values of the feature image in the $classes$ dimension are floating-point numbers between 0 and 1. Therefore, the adversarial model can determine the source of the current feature image only by judging whether the input segmentation feature image contains 0 and 1 or not. In order to solve this problem, on the one hand, the feature extraction of the original image is added, and the feature extractor (such as the first few layers in VGG) is used to extract the features of the image to obtain the first type of low-level features of the image. At the same time, because the segmentation image is a relatively abstract feature image that has undergone information extraction, using deep network will make the information loss more serious, so a shallower small network is used to transform it to obtain the second type of low-level features. Then the two types of low-level features will be merged and the CNN will be used for feature fusion. On the other hand, by scaling the one-hot feature map of the real segmentation image, the feature vectors of 0/1 are transformed into the feature vectors of floating point numbers. For the pixel i in the real segmented image, suppose its one-hot feature vector is v_i, and the feature vector after scaling is $\overline{v_i}$. At the same time, a fixed value ε is set, which means that the vector dimension (assuming the position is l) with the value of 1 in the feature vector cannot be less than ε after scaling. Meanwhile, obtain the feature vector u_i of the pixel at the same position in the generated segmentation image, then the value of the vector at position l in $\overline{v_i}$ is

$$\overline{v_i}^{l} = \max(\varepsilon, u_i^{l}) \tag{1}$$

, and the vector value of other position c in $\overline{v_i}$ is

$$\overline{v_i}^{c} = \frac{u_i^{c}(1-\overline{v_i}^{l})}{1-u_i^{l}} \tag{2}$$

Through the above scaling transformation, when the pixel category in the generated segmentation image is predicted correctly and the probability exceeds ε, the feature vector transformed by the pixels at the same position in the real segmented image will be exactly the same as the generated segmented image. If it is lower than ε, increase the probability value for other dimensions in proportion. These two operations further reduce the significant difference between the real segmentation map and the generated segmentation image and increase the difficulty to distinguish the true and false samples for adversarial network, and help the generation model to find the spatial continuity between pixels.

Table 2 The adversarial model structure table

Number	Type	The adversarial model
1	convolution	$[3\times3, 64]\times1$
2	convolution	$[3\times3, 128]\times1$
3	average pooling	$2\times2, stride=2$
3	convolution	$[3\times3, 256]\times1$
4	average pooling	$2\times2, stride=2$
5	convolution	$[3\times3, 512]\times1$
6	convolution	$[3\times3, 1]\times1$

In addition, in order to further enhance the distinguishing ability of the adversarial model, in the last layer, the size of the feature map is converted into a 4*4 judgment image, and each small grid represents the probability that the current region belongs to the real

segmentation image or the synthetic segmentation image. Performing a separate normalization operation on each small grid can prevent the global gradient adjustment of the feature image when the segmentation image only has a serious deviation in a certain part. Table 2 shows the detailed network structure of adversarial model.

2.4. Loss functions

During training, the generative network and the adversarial network will be trained separately to achieve the purpose of mutual confrontation and adjustment. Therefore, two loss functions need to be designed to be used in the training of the generative model and the adversarial model. In order to realize the adversarial idea of using models to compete with each other and increase alternately, when training a certain model, the weight of another model needs to be fixed.

For the generative model, a multi-category cross-entropy loss function is used to train the model to make a separate category judgment for each pixel. Assuming that the input image $H \times W \times 3$ is an RGB image x，the segmented image obtained after the transformation of the generation model is y . Therefore, the loss function of the separate training generative model is defined as follows.

$$loss_{mce}(y, y) = -\frac{1}{H \times W} \sum_{i=1}^{H \times W} \sum_{c=1}^{C} y_c^i \ln y \tag{3}$$

y is the one hot representation of the category the current pixel value belongs to. After training the generative model to convergence, introduce a adversarial model for training. In the adversarial model, when training the generative model, first input the image x into the generative model，then input the generated segmentation result $g(x)$ into the adversarial model together with the image x, and use the binary cross-entropy loss function to calculate the loss calculated by its confrontation result $d(g(x), x)$. The definition of the binary cross-entropy loss function is as follows：

$$loss_{bce}(z, z) = -[z \ln z + (1-z)\ln(1-z)] \tag{4}$$

The task of the generative model is to deceive the current adversarial model，so that it cannot distinguish the source of the segmented image input in the adversarial model, so the label of $g(x)$ is 1 (indicating that the source is real). Therefore, the loss function term of the adversarial model is $+loss_{bce}(1, d(g(x)))$, and according to the conclusion given in Goodfellow[8], using $-loss_{bce}(0, d(g(x)))$ can make the gradient descent of the generated model more stable when the adversarial model judges whether the source of the segmented image is real or synthetic. Therefore, the loss function of the training generative model is defined as follows：

$$loss_g = loss_{mce}(y, g(x)) - loss_{bce}(0, d(g(x), x)) \tag{5}$$

When training the adversarial model, since the adversarial model needs to distinguish whether the segmented image input in the model is real or synthetic, the segmented image synthesized by the generative model has a label of 0, and the segmented image that is actually obtained from the dataset has a label of 1. It is expected that the predicted value of the adversarial network can be close to 1 when the input segmented images are real, and the predicted value can be close to 0 when the input segmented images are synthesized. Therefore, the loss function of the training adversarial model is defined as follows.

$$loss_d = loss_{bce}(1, d(y, x)) + loss_{bce}(0, d(g(x), x)) \tag{6}$$

Therefore, for the training set containing N images, the segmented image corresponding to image x_i is y_i, the loss function of the entire model is defined as follows：

$$loss = \frac{1}{N} \sum_{i=1}^{N} loss_{mce}(y_i, g(x_i)) - \lambda[loss_{bce}(1, d(y_i, x_i)) + loss_{bce}(0, d(y_i, g(x_i)))] \tag{7}$$

In the formula, λ is a hyperparameter, which is used to adjust the loss size provided by the adversarial network in the initial training. Since the generation effect of the initial generation model is already good, but the adversarial model is still in the initialization state, the loss provided at this time is relatively large, so it needs to be adjusted by the hyperparameter to reduce the gradient size adjusted by the confrontation loss to the generation model.

3. Experiment

3.1. Dataset

There are two semantic datasets used for model testing in the experiment, namely PASCAL VOC 2012 and Cityscapes, both of which are currently commonly used semantic segmentation datasets. There are a total of 12031 images in the VOC 2012 dataset, and 1456 training images with semantic segmentation tags, 1449 test images, and 20 semantic segmentation categories. Because there are too few training pictures in VOC 2012 dataset, using VOC training network alone will lead to serious under-fitting, so it is necessary to use the SBD semantic segmentation dataset with 10582 sheets to supplement the dataset. Cityscapes is a large dataset containing a variety of stereoscopic video sequences recorded in street scenes from 50 different cities, which has 5000 high-quality pixel-level annotated pictures

and 20,000 rough-annotated pictures. In the experiment, the training set is 3475 images, and the test set is 1525 images, and there are 30 categories of images, and 19 categories are selected in the semantic segmentation task. Figure 4 shows some data samples of VOC 2012 dataset and Cityscapes datasets.

Fig.4 Samples of VOC and Cityscapes datasets

3.2. Evaluation indicators

All tables must be numbered consecutively (in Arabic numbers). Table headings should be placed (centered) above the table. Place tables as close as possible to where they are mentioned in the main text.

Intersection Over Union（IoU） is commonly used as an evaluation indicator in semantic segmentation, which means the coincidence degree between the predicted semantic label of the pixel and the semantic label of the labeled pixel (referred to as IoU), and the average coincidence degree of all categories (referred to as mIoU). The formula is defined as follows：

$$IoU(i) = \frac{p_{ii}}{\sum_j (p_{ij} + p_{ji}) - p_{ii}}$$
$$mIoU = \frac{1}{C}\sum_c IoU(c) \quad (8)$$

In the formula, p_{ii} indicates that the pixel is predicted to be of category i and the label is also of category i; p_{ij} indicates that the pixel is predicted to be of category i and the label is also of category j; p_{ji} indicates that the pixel is predicted to be of category j and the label is also of category i; C represents the number of categories of the dataset.

3.3. Training process

We uses Tensorflow deep learning framework in the experiment, and uses a NVIDIA TITAN GPU for training。

In training, the resolution of the input picture is 500*500, the data batch is set to 2, and the linear descent method is used to train 100,000 steps. In the training process, first train the generative model separately until the training reaches convergence. At this time, set the initial learning rate to 1e-4, and gradually attenuate to 1e-5. Then join the adversarial model for further training. Because the adversarial model is still in the initialization state, but the generative model is close to convergence at this time, so it is necessary to use a relatively large learning rate to help training the adversarial model. Generally, the learning rate of the generative model is reset to 3e-5, and the learning rate of the adversarial model is set to 3e-4. The parameter λ is set to 1e-2. In terms of optimization algorithms, the generative model uses the Adam optimizer, the adversarial model uses the Momentum optimizer, where the momentum is set to 0.9. In the experiment, VGG models are pre-loaded with the weights pre-trained with ImageNet, then the semantic segmentation dataset is used to train the segmentation task.

3.4. Experimental results and analysis

In the experiment, a total of 2 sets of experiments are set up, namely VGG16-8S and VGG16-8S-G, where G represents the using of a GAN structure in the segmentation model. By comparing the segmentation results whether the GAN is used in the image segmentation or not, we can find the effect of the GAN. The results on the PASCAL VOC dataset and Cityscapes dataset are shown in Table 3.

Table 3 Comparison tests of two segmentation models

dataset|network	VGG16-8S	VGG16-8S-G
PASCAL	71.62	73.18
Cityscapes	68.34	70.27

It can be seen from Table 3 that on the PASCAL VOC and Cityscapes datasets, the using of GAN can improve the segmentation accuracy of VGG16-8S to a certain extent. Among them, the IoU on PASCAL VOC increased by 1.56%. On the Cityscapes dataset, the IoU increased by 1.93%. The performance of VGG16-8S on the Cityscapes dataset is not as good as the PASCAL VOC dataset, the reason is that the images of the PASCAL VOC dataset are small, the original image size is only 500*375, and the number of segmentation objects is small and the size is small, so the tolerance to segmentation errors is higher. By introducing the GAN structure, the above defects can be improved, the segmentation can be more accurate, and the granulation phenomenon can be reduced, as shown in Figure 5.

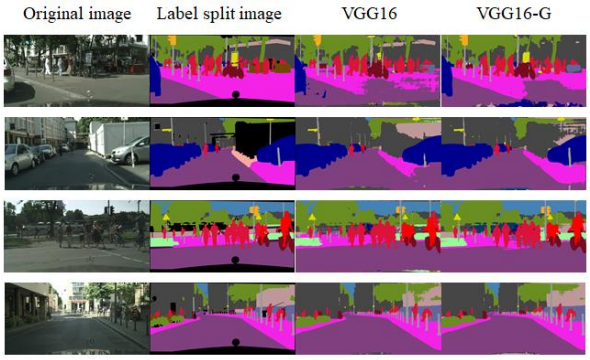


Fig.5 Samples of tests on the Cityscapes dataset

In Figure 5, it can be clearly seen that VGG16-8S are more prone to large-area loss and granulation on large objects such as roads, but after adding the GAN, it is significantly improved. In order to further compare the differences between the two models, 5 categories in the Cityscapes dataset were selected for IoU comparison in the experiment, as shown in Table 4.

Table 4 Comparison on the Cityscapes dataset

network	road	traffic	plants	pedestrian	vehicle
VGG16-8S	94.73	64.12	86.11	76.88	90.61
VGG16-8S-G	96.64	64.15	87.35	77.52	92.08

In Table 4, after introducing the structure of GAN，all types of segmentation accuracy have been improved to a certain extent. The categories which occupy a large area of the images such as roads, vehicles, etc. and have a large number of targets, the improvement effect is relatively good. However, for traffic lights, pedestrians and other categories with small area and small number, the promotion effect is weak. This is because small targets are difficult to be segmented, and information is easily lost in the preliminary filtering. Therefore, GAN improves the model's learning of pixel spatial continuity but is less helpful for segmenting small targets.

4. Conclusion

We introduce the GAN into the task of semantic segmentation to guide the existing semantic segmentation model to capture the binary potential function relationship between pixels. The segmentation effect is improved on the basis of the same model structure, parameters and calculation. Compared with the traditional method of using CRF and other post-processing techniques to improve the accuracy of segmentation model, it has a speed advantage. Through the experimental results on basic semantic segmentation models, VGG16-8S, it is also proved that the using of GAN can get a better effect to improve the segmentation accuracy.

References

[1] Long J , Shelhamer E , Darrell T . “Fully Convolutional Networks for Semantic Segmentation”, IEEE Transactions on Pattern Analysis & Machine Intelligence, vol 39, No.4, pp. 640-651, 2014.

[2] Krizhevsky A , Sutskever I , Hinton G . “ImageNet Classification with Deep Convolutional Neural Networks”. Advances in neural information processing systems, vol 25, No.2, 2012,.

[3] Szegedy C , Liu W , Jia Y , et al. “Going Deeper with Convolutions”. Proceeding of IEEE CVPR2015 Conference, Boston,pp.1-9, June.2015.

[4] Simonyan K , Zisserman A . “Very Deep Convolutional Networks for Large-Scale Image Recognition”. Computer Science, 2014.

[5] Silberman N, Hoiem D, Kohli P, et al. “Indoor Segmentation and Support Inference from RGBD Images”. 2012.

[6] Chen L C , Papandreou G , Kokkinos I , et al. “DeepLab: Semantic Image Segmentation with Deep Convolutional Nets, Atrous Convolution, and Fully Connected CRFs”. IEEE Transactions on Pattern Analysis & Machine Intelligence, vol 40, No. 4, pp:834-848, 2016

[7] Ronneberger O, Fischer P, Brox T. “U-Net: Convolutional Networks for Biomedical Image Segmentation”. International Conference on Medical Image Computing & Computer-assisted Intervention. 2015.

[8] Goodfellow I J, Pouget-Abadie J, Mirza M, et al. “Generative Adversarial Networks”. Advances in Neural Information Processing Systems. pp.2672-2680

[9] Liu Kexin(2000-),Undergraduate student，Her research interets include artificial intelligence and image processing.

[10] Guo Chenjun(1985-), Post-doctor ， Associate Researcher，His research interets include intelligent signal information processing.

JOINT SPARSE CONVOLUTIONAL CODING FOR IMAGE SUPER-RESOLUTION RESTORATION

SUN TAO[1], CHEN HUA WEI[1]

[1]School of Aeronautics and Astronautics, University of Electronic Science and Technology of China, Chengdu 611731, China
E-MAIL: suntao_0427@163.com, chenhuawei@uestc.edu.cn

Abstract:

The globality of the image is a strong constraint in the process of image super-resolution reconstruction. Convolutional sparse coding uses the global features of image in super-resolution reconstruction, and decomposes image wholly into convolution sum of filters and feature map instead of encoding the image patches. However, sparsity guided by the ℓ_1 norm cannot represent high-order structured information. In this paper, the joint sparse convolution coding (*JSCC*) proposed to further extract high-order structured information, leading to a compact dictionary. Our model involves the three sets of parameters to learn, the decomposition filters, mapping function and reconstruction filters. The model utilizes structured sparse regularization term $\ell_{2,1}$ regularization to constrain feature maps instead of single ℓ_1 norm. Meantime, extract edge prior information for registration with high frequency components. Extensive experiments demonstrate *JSCC* model can achieve competitive PSNR results, while reconstruction image illustrates better texture preservation performance and edge information. $\ell_{2,1}$ regularization term can also avoid the influence of noise, reflecting the superior robust performance.

Keywords:

Image super-resolution; Joint sparse convolutional coding; $\ell_{2,1}$ Norm regularization

1. Introduction

In the field of image processing, the resolution usually refers to the spatial resolution, and refers to the ability of the image acquisition system or display system to distinguish the details of the target object [1]. The spatial resolution of the image is determined by the sampling point interval on the image sensor, and an infinitely small sampling point corresponds to a pixel of the digitized image. Therefore, the spatial resolution of an image is the actual target size represented by one pixel.

In order to improve the spatial resolution of the image, there are two directions: hardware and software. In the hardware method, the array density can be increased by reducing the pixel size in the sensor [2], based on or increasing the chip size to improve the resolution of the imaging system. The method of using software to improve the image resolution refers to obtaining a higher resolution image through the image reconstruction algorithm without changing the imaging system. This method is usually also called image super-resolution (SR) reconstruction. Compared with the hardware method, the software-based method to improve the image resolution does not need to change the hardware structure of the existing imaging system, and the expansion capability is relatively low.

So far, many methods have modeled the prior knowledge of the local structure or patches of natural image [3]. Super-resolution process is a typical ill-posed problem, there are always multiple HR images corresponding to one LR image. Considering the complexity and local structure of the image in natural scenes, most single image super-resolution methods do not model the prior know-ledge of the entire image, but use the prior knowledge of image patches. A variety of classic SR methods, including prediction-based methods [5], edge-based methods [6], statistical methods [7], patches-based methods [8], and sparse representation methods [17] etc.

Gu et al. [9] firstly applied convolutional sparse coding to the single image SR problem, learning three sets of parameters through the training data set, LR dictionary, feature maps mapping function, and HR dictionary. Perform convolutional sparse coding modeling on the high-frequency components, and decompose the residual components into sparse feature maps with filters. Learn the mapping function from LR feature maps to HR feature maps.

Despite deep learning has been very effective in some low-level problems of computer vision, its physical interpretability has yet to be solved. In many research fields, it is a result-oriented black box. There is no clear and appropriate network structure design strategy. Therefore, we believe that

the study of traditional methods is still meaningful.

This paper applied the *JSCC* model on SR on the basis of convolutional sparse coding. Apply *JSCC* model to process high-frequency components and introduce structured sparse $\ell_{2,1}$ regularization terms. $\ell_{2,1}$ norm regularization for feature maps can represent the implied high-order structured information.

2. Joint sparse convolutional coding (*JSCC*)

The basic convolutional sparse coding problem is proposed in the form of Convolutional Basis Tracking Denoising (CBPDN), which is defined as:

$$\arg\min_{\{x_m\}} \frac{1}{2}\left\|\sum_m d_m \otimes x_m - s\right\|_F^2 + \lambda\sum_m \|x_m\|_1; \tag{1}$$

Where s is the input image of size $m \times n$, $\{d_m\}_{m=1,2,3,\cdots M}$ is a set of M-channel filters, $\otimes$ is convolution operator, $\{x_m\}_{m=1,2,3,\cdots M}$ is M-channel, $(m+s-1)\times(n+s-1)$ feature maps.

One solution to Eq (1) is to use the Alternating Direction Multiplier Method (*ADMM*) [10, 11] framework. Decompose Eq (1) into three sub-problems and alternatively solve the below optimization problem:

$$\{x_m\}^{(k+1)} = \arg\min_{\{x_m\}} \frac{1}{2}\left\|\sum_m d_m \otimes x_m - s\right\|_F^2 + \frac{\rho}{2}\sum_m \left\|x_m - y_m^{(k)} + \mu_m^{(k)}\right\|_F^2; \tag{2}$$

$$\{y_m\}^{(k+1)} = \arg\min_{\{y_m\}} \lambda\sum_m \|y_m\|_1 + \frac{\rho}{2}\sum_m \left\|x_m^{(k+1)} - y_m + \mu_m^{(k)}\right\|_F^2; \tag{3}$$

$$u_m^{(k+1)} = u_m^{(k)} + x_m^{(k+1)} - y_m^{(k+1)}; \tag{4}$$

These sub-problems are all univariate unconstrained optimization, which can be solved using conjugate gradient method or Newton method, also can transform to *Fourier* domain to solve [11].

Based on the sparse representation of the ℓ_1 norm neglects the structural characteristics and potential relationships between each variable. The single ℓ_1 norm which many papers used cannot encode these high-order structural information. Therefore, structured sparsity method proposed to handle this problem. In addition, relevant structural prior knowledge contributes to sparse representation reconstruction estimation. ℓ_1 norm as a measure of sparsity does not own scale-invariant property.

Above problem can be improved by structured sparsity method, the $\ell_{2,q}(q \in \{1,\infty\})$ norm can represent the information implicit in the sparsity mode of the signal, and get better sparse approximation. $\ell_{2,q}(q \in \{1,\infty\})$ norm induces the sparsity regularization term, which can encode the high-order structured information implicit in the sparsity mode of the signal, thereby obtaining a better sparsity approximation.

The *JSCC* model [4] is expressed as:

$$\arg\min_{\{x_{c,m}\}} \frac{1}{2}\sum_c \left\|\sum_m d_m \otimes x_{c,m} - s_c\right\|_F^2 + \lambda\sum_c\sum_m \|x_{c,m}\|_1 + \mu\left\|\{x_{c,m}\}\right\|_{2,1}; \tag{5}$$

Where x is the m-dimensional, c-channel feature maps, $\|x\|_{2,1}$ is the $\ell_{2,1}$ norm of x, $\|x\|_{2,1} = \sum_{l=1}^{N}\|x_l\|_2$, $\|x_l\|_2 = \sqrt{\sum_{j=1}^{n}|x_{i,j}|}$, as shown in Figure 1. $\ell_{2,1}$ norm constraint makes feature maps sparse in the row direction. Meanwhile each nonzero value sparse vector acquired at the same sparse mode. There are already evidences [12, 13] that for the expression of the system, most of the parameters are unnecessary for the improvement of reconstruction accuracy, and row sparsity reduces the number of parameters of the system, but does not affect the final accuracy of reconstruction.

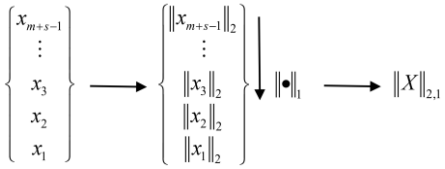


Fig.1 $\ell_{2,1}$ mixed norm

3. *JSCC* model for SR

Similar to most existing single image super-resolution methods, the *JSCC* model architecture also involves training phase and test phase. In the training phase, three sets of parameters need to be learned: (1) decomposition filter, (2) mapping function between LR/HR feature maps, (3) reconstruction filter. Our *JSCC* model architecture is shown in Figure 2.

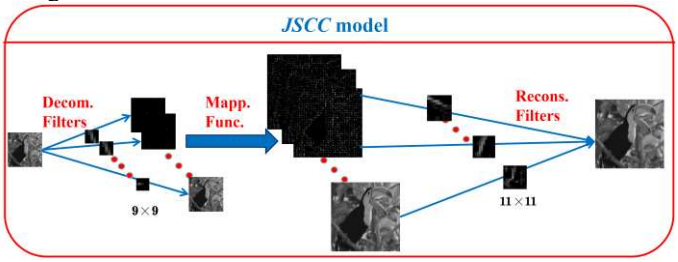


Fig.2 The training/testing phase

The decomposition filter is trained through the train set, and the HR sparse features are predicted by the LR sparse feature maps through the mapping function. Subsequently, train a filter that can sparsely express the data set to generate sparse feature maps, and can also generate sparse feature

maps for samples of the same type.

3.1. Decomposition filters

HR images are expressed as $\{x_1, x_2, \cdots x_M\}$, and LR images are noted as $\{y_1, y_2, \cdots y_M\}$. The LR image and HR image are highly correlated. Therefore, decompose the LR image into smooth components and residual components, and only learn the residuals between LR/HR images.

On account of extracting the feature information as prior information is the important part. The more prior knowledge extracted, the more accurate the prediction of the missing HR information. The first derivative used to extract the feature information can only obtain the feature of horizontal and vertical feature. Meantime, convolution operation will make the reconstruction result too smooth, so we add the Sobel edge operator to better register with the high-frequency component.

$$\begin{aligned} &\min_X \left\| y - d^s \otimes X_y^s \right\|_F^2 + \eta \left\| d^h \otimes X_y^s \right\|_F^2 \\ &+\eta \left\| d^v \otimes X_y^s \right\|_F^2 + \eta \left\| d^e \otimes X_y^s \right\|_F^2; \end{aligned} \tag{6}$$

Where y, X_y^s, η are residual component, LR sparse feature maps, regularization parameters respectively, d^s, d^h, d^v, d^e are low-pass filter, horizontal filter [1, -1], vertical filter [1; -1] and Sobel edge filter respectively.

$$y = d^S \otimes X_y^s + Y; \tag{7}$$

Y is the residual component of LR images. Decompose the residual components into N-dimensional feature maps:

$$\begin{aligned} &\min_{X,d} \left\| Y - \sum_{i=1}^N d^l \otimes X_i^l \right\|_F^2 + \lambda \sum_{i=1}^N \left\| X_i^l \right\|_1 + \mu \left\| X \right\|_{2,1}; \\ &s.t. \ \left\| d_i^l \right\|_F^2 \le 1 \end{aligned} \tag{8}$$

Where λ, μ are regularization parameters, Eq (8) can alternately optimize under *ADMM* frame [10-11].

3.2. Mapping function and reconstruction filters

HR images adopt the same decomposition strategy. Z is the residual component of the HR image. The key part of the SR reconstruction lies in establishing the mapping function between LR images and HR images, the joint learning reconstruction filter and mapping function is modeled as:

$$\begin{aligned} &\{d^h, W\} = \min_{d,W} \left\| Z - \sum_{j=1}^M d_j^h \otimes g(d^l; w_j) \right\|_F^2; \\ &s.t. \ \left\| d_j^h \right\|_F^2 \le e \ ; \ w_j \ge 0, \left| w_j \right| = 1 \end{aligned} \tag{9}$$

e is a scalar, used to constrain the energy of the reconstruction filter. In order to maintain the consistent sparsity of LR feature maps and HR feature maps, linear transformation is applied to estimate HR feature maps. The mapping function $g(d^l(x,y); w_j) = w_j^T d^l(x,y)$ can maintain the distribution of the output and the LR feature maps. The filter and mapping function can be optimized alternately in Eq (9).

If HR feature maps are convolved directly with reconstruction filters, the image texture and edge information will be obtained, as shown in Figure 3.

For the fixed W and optimized sub-problems d^h,

$$\begin{aligned} &\{d^h\} = \arg\min_W \left\| X - \sum_{j=1}^M d_j^h \otimes g(d^l; w_j) \right\|_F^2; \\ &s.t. \left\| d_j^h \right\|_F^2 \le e \end{aligned} \tag{10}$$

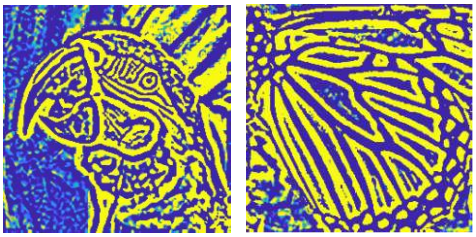


Fig.3 HR sparse feature maps convolution with reconstruction filters

Above univariate optimization problem with inequality constraints can utilize external point penalty function method, the objective function is:

$$\begin{aligned} &P(W, m) = \left\| X - \sum_{j=1}^M d_j^h \otimes g(d^l; w_j) \right\|_F^2 \\ &+m[\min(0, (g_j)^2]^2; g_j = -\left\| d_j^h \right\|_F^2 + e \end{aligned} \tag{11}$$

m is the penalty parameter, and specific solutions can refer to [14]. For fixed d^h, W, sub-problems are more complex, following optimization problem needs to be solved:

$$\begin{aligned} &\{W\} = \arg\min_W \left\| X - \sum_{j=1}^M d_j^h \otimes g(d^l; w_j) \right\|_F^2; \\ &s.t. \ w_j \ge 0, \left| w_j \right| = 1 \end{aligned} \tag{12}$$

Eq (12) can using the *SA-ADMM* algorithm [9].

3.3. The testing phase

In the testing phase, LR sparse feature maps X^l use the mapping function to predict HR feature maps. HR image texture and high-frequency component are obtained by $X = \sum_{j=1}^M d_j^l \otimes X_j^h$. The back-projection operation has been used in many papers [15-16]. This paper also utilizes this strategy to improve the reconstruction results.

4. Experiments

In this Section, we will demonstrate the reconstruction

results of *JSCC* method. LR images are degraded from high-resolution datasets through down-sampling and blurring. *BSDS300* with training images is used for our model training. When testing the SR performance of the model, PSNR on the Y channel after converting to YCbCr channels is used to quantitatively evaluate the reconstruction quality. We select public datasets Set14 as test images.

4.1. Parametric analysis

In fact, image features are scattered in filters and feature maps of different dimensions. Thus, a large size filter can improve the information representation capability when the number of feature maps is fixed. we increase receptive field area, and set decomposition filters size and reconstruction filter size to 9×9 and 11×11 respectively.

Obviously, filters dimension is a key parameter. filters number in this paper is essentially the minimum number of freedom degrees needed to sample a specific image that meets the structured sparsity. In general, on account of the sparser the feature maps after image sampling, the lower the cost of the transmission process, but the dimension and atoms number of filters in the reconstruction process should be as large as possible, thereby algorithm complexity of the reconstruction process is higher.

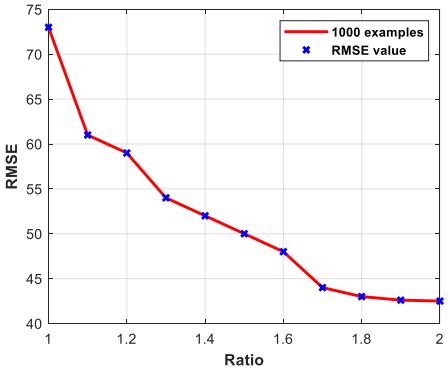


Fig.5 Reconstruction error and N to M ratio

We verify the effect of using different filter numbers on the reconstructed image, and choose an appropriate ratio between the number of decomposition filters N and the number of reconstruction filters M. Set the initial number of decomposition filters N to 100, and set the ratio between the number of decomposition filters and reconstruction filters to 1 to 2. We select 1000 training images, and dynamically select the number of reconstruction filters M according to the step size of 0.1 times. The relationship between RMSE and ratio is shown in Figure 5.

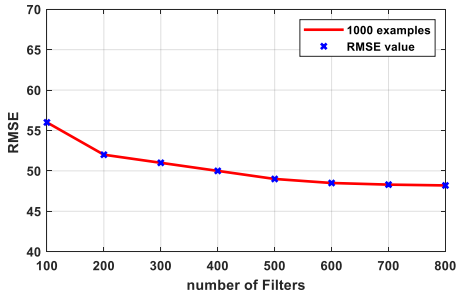


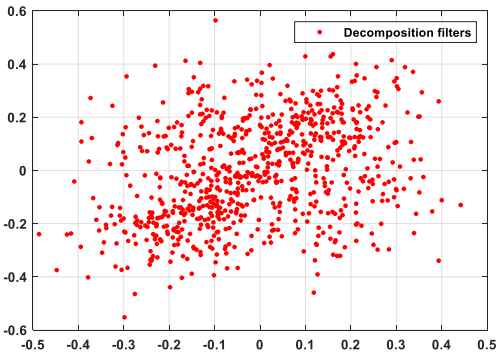
Fig.6 Number of filters and reconstruction error

As shown in Figure 5 and Figure 6, When the ratio of M to N is 1.8, RMSE tends to converge. reconstruction filters number should be 1.8 times the number of decomposition filters. So we set decomposition filters number to 800, and the reconstruction filters number should be 1440. About other parameters selection, the parameters of the regularization term, we set manually λ is 20 and μ is 1.5.

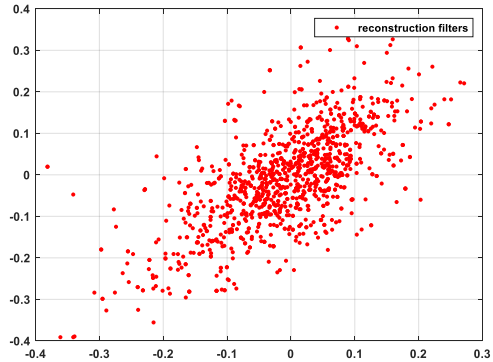
4.2. Correlation between different dimensions filters

Generally, feature maps can view as low-dimensional projections of high-dimensional space. the more the number of decomposition filters and reconstruction filters, the more sufficient features information can be expressed. If the similarity between different filters dimensions is greater, it means that image hold more redundant information. The smaller the similarity between the filters, indicating the more complex the structure of the image. Therefore, encoding the feature information requires a large number of filters, and the decoding cost is also relatively high.

We examine the similarity between the decom-position filter and the reconstruction filter, and stretch the size $m\times n\times c$ filter into $mn\times1\times c$ dimensional vector, where c is number of channels. We perform K-means clustering algorithm analysis on the filters. As shown in Figure 7, the filter distribution is concentrated in the area, illustrating that most of the decomposition filters of different dimensions are similar, and the energy is concentrated in the expression of certain features. It shows that the residual components of the image contain high-frequency components (edges, corners, textures) and other features. Within a certain error range, a set of sparse feature maps can be used to reconstruct the high frequency components in general. The distribution of reconstruction filters and decomposition filters in Figure 7 are roughly the same in energy concentration area, but distribution is different. It also shows the conversion from LR space to HR space for the mapping function.



(a) Decomposition filters



(b) Reconstruction filters

Fig.7 Distribution of decomposition filter and reconstruction filter

4.3. The robustness of $\ell_{2,1}$ regularization

$\ell_{2,1}$ regularization has strong anti-interference ability against signal singular values and noise. In order to verify the robustness of our model, we add Gaussian mixture noise to the training set and test the influence on Set14.

We weight Gaussian noise with different variances into mixed Gaussian noise. Gaussian mixture noise $G(x)=(1-C)*G(0,\sigma_1^2)+C*G(0,\sigma_2^2)$, $G(0,\sigma_i^2)$ is Gaussian probability density function with zero mean and variance is σ_i^2 , Consider here that the noise has a fixed variance, and we set manually $\sigma_1=0.2$, $\sigma_2=2$. C is a constant that controls the noise amplitude.

Perform mixed Gaussian noise processing on 50% of the data set, and image contaminated by mixed Gaussian noise viewed as interference data. Taking the zooming factor of 3 as an example, the PSNR results of reconstruction by different algorithms are shown in the Table 1. Table 1 illustrates that with the increase of the noise amplitude, from the perspective of PSNR value, the interference data is almost negligible for model processing.

Table 1 Average PSNR after adding different amplitude noise

C (Noise amplitude)	Average PSNR (dB)
C = 0	29.15
C = 0.02	29.15 ± 0.03
C = 0.04	29.15 ± 0.07
C = 0.06	29.15 ± 0.09
C = 0.08	29.15 ± 0.11
C = 0.1	29.15 ± 0.25

4.4. PSNR results

The PSNR values of Set14 are shown in Table2, 3. The reconstruction effect of *JSCC* model performs better in most test images. Taking a zooming factor of 3 as an example. We compare *JSCC* with traditional methods and deep learning methods, using the classic sparse coding super-resolution ScSR [17] model, and SRCNN [19], DBPN [15], and VDSR [18] in deep learning as comparisons. Average PSNR results indicate 1.3 dB higher than ScSR. And average value of *JSCC* model are close to the DBPN based on dense connections and VDSR based on residual network structure.

Table 2 The PSNR results with different algorithms

Zooming factor of 3 (dB)					
Set14	**ScSR**	**SRCNN**	**VDSR**	**DBPN**	***JSCC***
baboon	23.11	23.59	23.76	**23.79**	23.29
barbara	26.07	26.65	26.81	26.75	**26.94**
bridge	25.04	25.07	25.12	25.09	**25.20**
face	33.11	33.57	33.60	33.72	**33.80**
coast	26.80	27.19	27.35	**27.47**	27.27
comic	23.58	24.38	24.45	24.46	**24.52**
flowers	27.83	28.97	29.13	29.43	**29.52**
foreman	29.95	33.34	33.98	33.75	**34.24**
lena	32.16	33.39	33.42	33.47	**33.62**
man	27.45	28.17	28.12	28.23	**28.34**
monarch	30.17	31.38	31.47	**31.65**	31.08
pepper	31.10	34.34	34.48	34.56	**34.72**
zebra	27.41	28.86	**29.33**	29.22	29.30
ppt3	25.58	26.02	26.24	26.13	**26.32**
average	27.81	28.92	29.08	29.12	**29.15**

Despite our model fails to greatly surpass the PSNR result achieved by existing deep learning model, we optimize the different parameters in stages rather than end to end mapping strategies. our model has a clear structure and good interpretability. Reconstruction images are shown in Figure 8, 9, In order to compare the results of different algorithms, the content in the red box is the enlargement of a local area of the reconstructed image. As a whole, results demonstrate

our algorithm can better preserve texture and high-frequency detail components.

Table 3 The PSNR results with different algorithms

Zooming factor of 2 (dB)					
Set14	**ScSR**	**SRCNN**	**VDSR**	**DBPN**	***JSCC***
baboon	25.03	25.73	26.27	**26.35**	26.13
barbara	28.70	28.59	**29.47**	29.05	29.43
bridge	27.65	27.70	27.57	27.63	**27.83**
face	35.69	35.60	35.70	32.19	**35.73**
coast	30.06	30.81	30.53	29.06	**30.82**
comic	28.02	28.28	29.02	**29.17**	28.52
flowers	32.73	33.04	33.91	**34.19**	33.31
foreman	36.79	36.19	36.45	35.52	**36.47**
lena	35.46	36.48	36.19	36.06	**36.63**
man	30.07	30.82	**31.23**	31.07	30.82
monarch	35.33	37.74	37.98	**38.40**	38.15
pepper	36.72	35.87	36.76	36.84	**36.88**
zebra	33.43	33.49	33.23	**33.77**	33.50
ppt3	28.58	31.52	31.76	31.33	**31.95**
average	31.73	32.27	32.57	32.18	**32.66**

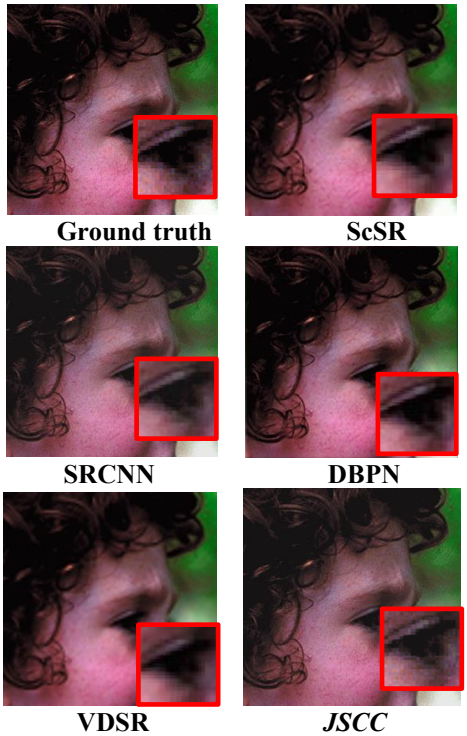


Fig.8 SR on image *face* by different algorithms, (Zooming factor of 3)

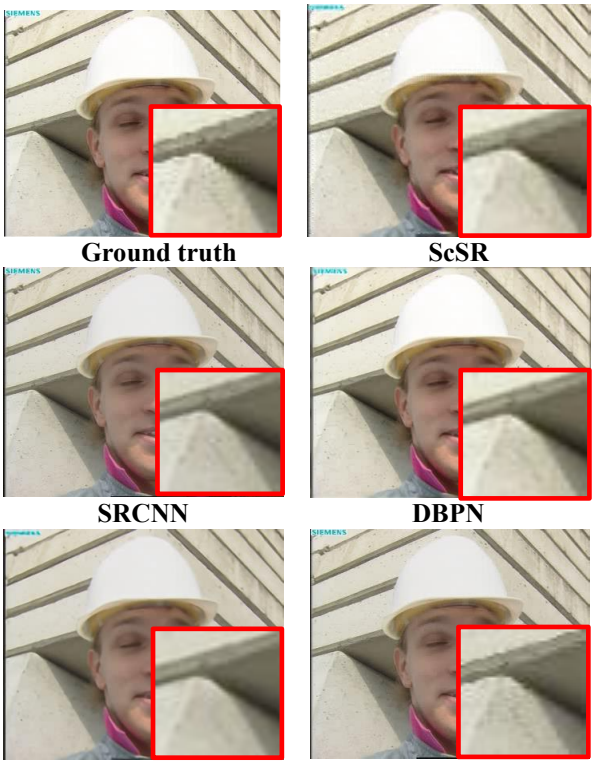


Fig.9 SR on image foreman by different algorithms, (Zooming factor of 3)

5. Conclusions

This paper applied the joint sparse coding method to image super-resolution, optimizing three groups of parameters in training phase, decomposition filter, reconstruction filter and mapping function. *JSCC* uses $\ell_{2,1}$ norm regularization term to extract high-order structured high-frequency components, and $\ell_{2,1}$ norm can overcome the shortcoming that a single ℓ_1 norm cannot represent high-order structural information. In order to improve the over-smooth effect of the reconstructed image caused by the convolution operation, we exploit the edge prior information to better register with the high-frequency components. Experimental results show that the *JSCC* reconstruction method can better preserve high-frequency details and texture. *JSCC* can also increase the robustness of the system and suffer less interference from the noise.

References

[1] Z. Wang, J. Chen, and S. C. Hoi, "Deep learning for

image super-resolution: A survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 2020.

[2] L. Yue, H. Shen, J. Li, Q. Yuan, H. Zhang, and L. Zhang, "Image super-resolution: The techniques, applications, and future," *Signal Processing,* vol. 128, pp. 389-408, 2016.

[3] Y. Chen, R. Ranftl, and T. Pock, "Insights into analysis operator learning: A view from higher-order filter-based mrf model," *IEEE Trans. Image Process,* vol. 23, no. 3, pp. 1060-1072, 2014.

[4] X.-T. Yuan, X. Liu, and S. Yan, "Visual classification with multitask joint sparse representation," *IEEE Transactions on Image Processing,* vol. 21, no. 10, pp. 4349- 4360, 2012

[5] T. Guo, H. Seyed Mousavi, T. Huu Vu, and V. Monga, "Deep wavelet prediction for image super-resolution," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2017, pp. 104-113.

[6] J. Xie, R. S. Feris, and M.-T. Sun, "Edge-guided single depth image super resolution," *IEEE Transactions on Image Processing,* vol. 25, no. 1, pp. 428-438, 2015.

[7] Z. Xiong, X. Sun, and F. Wu, "Robust web image/video super-resolution," *IEEE transactions on image processing,* vol. 19, no. 8, pp. 2017-2028, 2010.

[8] W. T. Freeman, T. R. Jones, and E. C. Pasztor, "Example-based super-resolution," *IEEE Computer graphics and Applications,* vol. 22, no. 2, pp. 56-65, 2002.

[9] S. Gu, W. Zuo, Q. Xie, D. Meng, X. Feng, and L. Zhang, "Convolutional sparse coding for image super-resolution," in *Proceedings of the IEEE International Conference on Computer Vision* ,pp. 1823-1831, 2015.

[10] S. Bhaskar and W. Zou, "An ADMM solution to the sparse coding problem," 2011.

[11] B. Wohlberg, "Efficient algorithms for convolutional sparse representations," *IEEE Transactions on Image Processing,* vol. 25, no. 1, pp. 301-315, 2015.

[12] V. Sze, Y.-H. Chen, T.-J. Yang, and J. S. Emer, "Efficient processing of deep neural networks," *Synthesis Lectures on Computer Architecture,* vol. 15, no. 2, pp. 1-341, 2020.

[13] M. Denil, B. Shakibi, L. Dinh, M. A. Ranzato, and N. De Freitas, "Predicting parameters in deep learning," in *Advances in neural information processing systems*, pp. 2148-2156, 2013.

[14] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[15] M. Haris, G. Shakhnarovich, and N. Ukita, "Deep back-projection networks for super-resolution," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 1664-1673, 2018.

[16] Y. Zhu, Y. Zhang, and A. L. Yuille, "Single image super-resolution using deformable patches," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, , pp. 2917-2924, 2014.

[17] J. Yang, J. Wright, T. S. Huang, and Y. Ma, "Image super-resolution via sparse representation," *IEEE transactions on image processing,* vol. 19, no. 11, pp. 2861-2873, 2010.

[18] J. Kim, J. Kwon Lee, and K. Mu Lee, "Accurate image super-resolution using very deep convolutional networks," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 1646-1654, 2016.

[19] C. Dong, C. C. Loy, K. He, and X. Tang, "Learning a deep convolutional network for image super-resolution," in *European conference on computer vision*, 2014, pp. 184-199: Springer.

A MULTI EXPOSURE SYNTHETIC HDR IMAGE ALGORITHM BASED ON CASCADED NETWORK

YU LI[1], WU RUI[1], HE JIAN[2]

[1] School of Automation, University of Electronic Science and Technology of China, 611731, Chengdu, China
[2] Yibin Institute, University of Electronic Science and Technology of China, Yibin, China
E-MAIL: lyu@uestc.edu.cn, 690784043@qq.com, hejian@uestc.edu.cn

Abstract:

At present, the large challenge of synthesizing HDR (high dynamic range) images from multiple exposure images is the problem of artifacts caused by moving objects and camera shake in dynamic scenes. In this paper, a three-layer cascaded network structure of HDR image generation method is proposed. With the deepening of the network, images with different exposure levels are input for processing. Each sub network only converts and extracts the feature of one exposure level image. Finally, a gradually improved HDR image is obtained through the cascaded structure. Through this cascaded network processing, the mutual interference and confusion of dynamic regions between multiple images can be reduced. Compared with the existing HDR generation methods, this method can solve the problem of artifacts and keep the texture details of the generated HDR image well.

Keywords:

Cascaded network; HDR image; Artifacts; Multiple exposure image

1. Introduction

The multi exposure synthetic HDR image method is the most widely used and well researched method for high dynamic range image generation. The basic idea of synthetic HDR image method is to use LDR (low dynamic range) image acquisition equipment to take multiple pictures of the same scene with different exposure parameters, and then fuse these images according to a certain method. Each LDR image records the different range of the scene radiation value. The overall brightness of the underexposed image is low, showing the details of the high bright area. While the overall brightness of the overexposed image is high, which improves the information visibility of the dark area. When there are no moving object, displacement of the scene or camera shake, pixel level fusion method can be carried out directly. For example, the hybrid weight algorithm proposed by Debevec [1] can achieve good results for HDR synthesis. However, when there is a small displacement of the scene, or there are moving objects in the scene, the synthetic HDR image will have artifacts.

The traditional image processing method is based on the fusion of image domain, which depends on the alignment state of images, so it is difficult to avoid artifacts. Deep learning method can learn dynamic region reconstruction from a large number of samples, and has excellent performance in complex mapping tasks. Therefore, neural network has unique advantages for multi exposure images of HDR image synthesis.

Kalantari [3] first applied convolution network to multi frame HDR image fusion strategy. His reconstruction does not entirely rely on convolution network, but uses optical flow method for image registration of multi frame images with moving foreground to make the contents of multiple images consistent as far as possible, and then input the aligned multi frame images into a lightweight network. However, the artifact problem still exists due to the optical flow method. Wu [4] proposed a CNN network, which can extract and fuse the high-dimensional features of three different exposure images at the same time. Compared with Kalantari's method, this method realized the end-to-end mapping of LDR to HDR image completely with the help of convolution network. They do not use any traditional HDR synthesis strategy, which can solve the problem of artifacts to a certain extent, but there are still some deficiencies in the texture details of the generated image.

In order to solve these problem, a three-level network model is designed in this paper. The LDR images with different exposure levels are input sequently to the network. The reference frame images are processed preferentially by the first layer branch, which effectively avoids the mixed artifacts caused by the foreground displacement. Then, the second branch and the third branch extract the over light and dark information contained in the low exposure image and the high exposure image step by step. The three sub network branches share the difficulty of multi frame HDR generation, which not only solves the problem of image artifacts

generated by HDR image synthesis, but also guarantee the quality of the output image.

2. Three-layer cascaded network structure of HDR image synthesis

In the multi exposure HDR generation task, three LDR images with different exposure levels are generally used as input. Among them, the image with medium exposure level can show most of the dynamic range of the scene, and the final output HDR needs to be consistent with the medium exposure image content, so the medium exposure image is generally referred to as the reference frame. Meanwhile, images with lower and higher exposure levels focus on the image content at both ends of the dynamic range.

Our method takes the UNET encoder decoder model as the sub network structure in the cascaded network. Three UNET networks of the same structure are connected end to end, and the LDR images with medium, low and high exposure levels are sequently input to the multi exposure HDR synthesis network. Each level of UNET takes an LDR image and the output of the superior branch as the input of the sub network, and the LDR image features are extracted through convolution and deconvolution operations. During this processing, the LDR image is transformed into higher level image features. The image information (such as image content, light intensity, texture details, etc.) required by the multi exposure image fusion algorithm is extracted in the encoding process. The decoder restores the image according to these information, and expands the dynamic range according to the characteristics of HDR image. The overall network structure is shown in Figure 1.

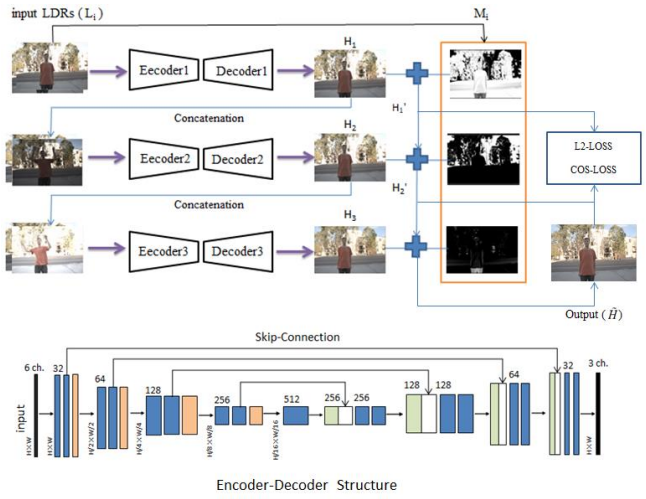


Fig.1 Diagram of three layer cascaded network for HDR synthesis

To maintain the local contrast, the HDR image was synthesized step by step. In the first branch, the medium level exposure image L_1 is taken as the key conversion object, and two identical L_1 images are used as the initial input. The distribution of LDR to HDR data is quite different and it is difficult to learn. Therefore, the main function of the first layer coding and decoding network branch is to complete the basic conversion from LDR data domain to HDR data domain, that is, the range of 0 to 255 of LDR data is expanded to the range of high dynamic range.

After the 1st layer network, a relatively rough HDR image H_1 is obtained. Although H_1 is close to the high dynamic range image in numerical value, it is only limited to middle level of the brightness. Then H_1 superimposed with the low-level exposure image L_2 are input into the second layer sub network. The output of the second branch H_2 can modify the low dynamic range image content based on the first branch. Specifically reflected in the second branch output image in the high brightness area can be closer to the HDR image, the contrast and color of the underexposed area are further restored.

Finally, the 2nd branch output H_2 is superimposed with the high-level exposure LDR image L_3, which is similar to the previous layer. Through the processing of the third branch, the image content, texture details and color of the low brightness level are enhanced, and the output H_3 of the third layer is obtained.

The outputs of three branches are not directly used as the final HDR estimation image, but they are fused by means of weighted graph. The weighted graph is a matrix with the same size as the input image. The purpose is to extract the overexposed, underexposed and medium brightness areas in the scene respectively. Thus, three weight matrices corresponding to three exposure levels are obtained.

The weighted graph is calculated from the reference frame image, which reflects the areas of the image corresponding to the exposure level.

First of all, it is necessary to normalize the reference frame LDR image L_1, and then use equation (1) to calculate the brightness map I of the image.

$$I(x)=0.299L_{1,r}(x)+0.587L_{1,g}(x)+0.114L_{1,b}(x) \tag{1}$$

According to the formula (2), the weight map M_3, M_2, M_1 corresponding to the high, low, middle level exposure image are calculated. The threshold t_a and t_b represents the degree of darkness and brightness respectively, where the value is 0.2 and 0.9.

$$M_1(x)=1-M_2(x)-M_3(x)$$

$$M_2(x)=\frac{\max\left(I_1(x)-t_b,0\right)}{t_b}$$

$$M_3(x) = \frac{\max\left(I_1(x) - t_a, 0\right)}{1 - t_a} \tag{2}$$

The weighted fusion results of each branch output are calculated as follows, and the final HDR image is obtained through the transmission and fusion of output layers:

$$H_1' = H_1 \cdot M_1 + L_1(1 - M_1) \tag{3}$$

$$H_2' = H_2 \cdot M_2 + H_1'(1 - M_2) \tag{4}$$

$$H_3' = H_3 \cdot M_3 + H_2'(1 - M_3) \tag{5}$$

The loss function of the network L_{unet} is shown as formula (6):

$$L_{unet} = L_m + \lambda L_c \tag{6}$$

Here L_{m} is the pixel value loss, and we use L2 loss to calculate it. L_{c} is color accuracy loss, we use cos loss to represent it. λ is the weight of cos-loss.

The loss value of the whole network L_{w} can be obtained by calculating the average value of each layer L_{unet}^{j} (j=1,2,3).

$$L_w = \frac{1}{3}\sum_{j=1}^{3}(L_{unet}^{j} \cdot M_j) \tag{7}$$

3. Experiments results

3.1. Datasets

To test the effectiveness of our method, we select four databases. One is Kalantari's dataset [3], which is used as training samples. It has 74 scenes, and each scene includes three images with equal interval of exposure levels. The camera is basically aligned, and most of the foreground characters have displacement. According to the input size of the network, we resize all the images to 256 × 256. With simple data enhancement operations, such as rotation and flip, we obtain 43000 image groups, and each group contains three LDR and one HDR images.

The second dataset provided by Sen [6] contains 30 different scenes, which are composed of three or more LDR images with different exposure levels, most of which have slight foreground movement.

The third dataset provided by Tursun [7] consists of 9 LDR images of each scene, and the exposure horizontal span is relatively small. Compared with Sen's dataset, this dataset has larger foreground movement, lower alignment and more difficult HDR synthesis. It is a difficult sample to test HDR image generation and artifacts removal methods.

The fourth dataset is EMPA [8]. The images captured in EMPA dataset are mainly landscapes in static scenes, which are quite different from other datasets in texture and hue. The images are aligned and can be used to evaluate whether the reconstruction effect of network model is satisfactory visually.

3.2. Evaluation standard

This paper uses HDR-VDP-2.2[9] standard to assess the HDR images quality. It provides a probability graph to visualize the probability of visual difference of each pixel (vdp) and the quality score of the HDR image.

3.3. Objective evaluation

The objective evaluation standard directly shows the difference between the estimated HDR image and the real image, and the result needs to be calculated on the image sample with real label. Twenty five LDR-HDR image sets were randomly selected from Kalantari and EMPA datasets to calculate the scores. We compare our method with two traditional multi frame methods: Debevec [1] and Mertens [2]. In addition, we also implement two HDR image reconstruction methods based on deep learning, which is the code and decode fusion model proposed by Wu [4]. And a single frame HDR reconstruction network named Exp-net proposed by Marnerides [5]. Table 1 shows the quality score calculated by the above four methods and our method (C-net), and the bold values in the table represent that the best results.

As shown in Table 1, our method performs the best, and the quality score of the synthetic HDR image is the highest. The detection probability map output from hdr-vdp-2.2 can also show which areas of the image have great visual difference. Figure 2 shows the detection probability map of HDR estimated by various methods in a test scene. The red area represents the obvious difference with the ground truth (GT). And the blue color means that the difference is difficult to see. The blue region of our method is the largest, which indicate that the HDR estimation graph of the output of the C-net (ours) is closest to the ground truth.

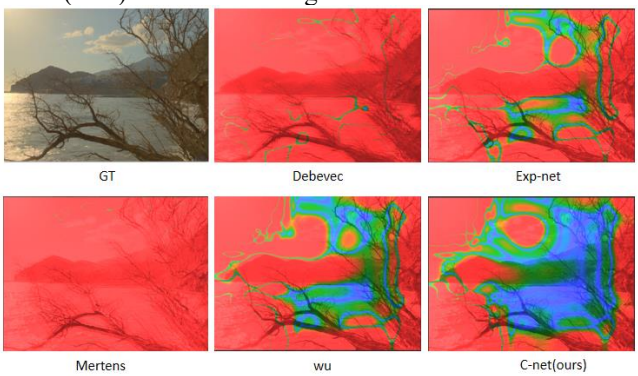


Fig.2 Comparison of vdp of HDR-VDP-2.2

Table 1 Comparison of the quality score

	De-bevec	Mer-tens	Wu	Exp-net	C-net (ours)
HDR-VDP-2.2	62.19	63.35	65.42	62.92	**66.36**

3.4. Subject evaluation

The following is the comparison of HDR generation effect between the existing methods and our method. Figure 3 shows the artifact remove effect of various methods in dynamic scene.

It can be seen that in the process of multi exposure image shooting, the foreground object is in dynamic state, resulting in the change of the pose and angle between the images. Traditional exposure fusion methods Debevec and Mertens produce serious artifacts, and the quality of HDR image is poor. The deep learning methods including C-NET can effectively avoid this problem. Because Exp-net only extracts information from the reference frame, the HDR image performance is poor, which is mainly reflected in the low contrast of object details, such as the loss of clothing texture and the inability to recover the color of the background sky. Wu and our method are the closest to the real HDR image. It can be seen from the Figure 3 that all the details of the generated image are relatively perfect, and the color is more accurate and natural.

It can be concluded that compared with the traditional image processing, the deep learning method can learn the HDR fusion in dynamic scene from a large number of samples. This process can avoid the artifacts, overlapping and confusion caused by image misalignment.

Fig.3 Comparison of anti-artifact performance

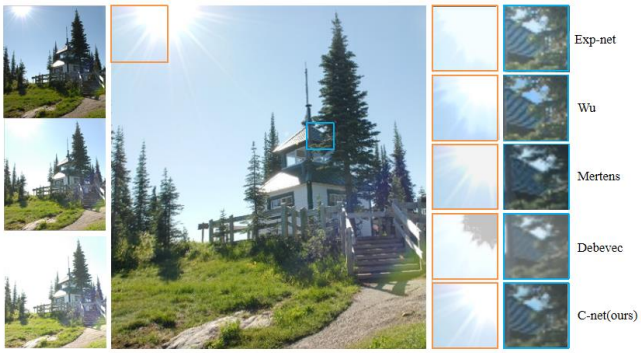


Fig.4 Repair comparison of overexposed and underexposed areas

C-net can not only effectively avoid artifacts, but also maintain high quality synthesis of HDR images. Figure 4 shows the comparison of the detail repair effect through local magnification. There is only slight shake in the scene. The difficulty of HDR reconstruction is not artifact, but how to repair the underexposed and overexposed area in LDR image. As showed in Figure 4, because the sunlight is the brightest in the scene, the pixel value of the surrounding area is compressed to a relatively narrow range. The right side of Figure 4 shows the local repair effect of several methods. It can be seen that except for Mertens and our methods, other methods have produced unnatural gradients in the sunlight. Exp-net and Wu methods are not smooth at the transition of the light, and produce similar rendering artifacts, and lose the texture of scattered rays. Debevec method even produces dark spots.

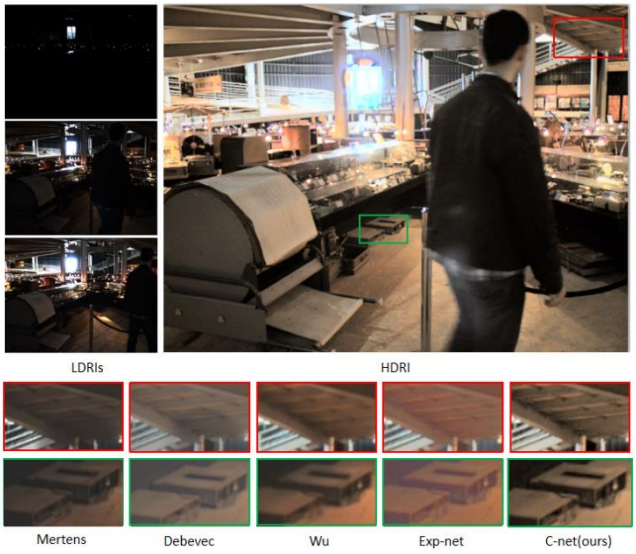


Fig. 5 Comparison of texture detail

Another block diagram shows the details of the shadows. In the images generated by Mertens and Debevec methods,

the texture of buildings becomes blurred and the contrast of deep and light stripes is poor, while our method can retain the texture detail. From all above, our method achieves good results in both cases.

Figure 5 shows a relatively difficult sample, which comes from the Tursun dataset. Among them, the exposure values between multiple LDR images vary widely with large foreground displacement and poor light, thus it is difficult to extract effective features from the image. It can be seen that the output of Mertens' method is still at a low brightness, and the details of dark area are not highlighted to be clear. While Debevec and Exp-net methods cannot expand enough dynamic range to show the local bright and dark details well. And the two traditional methods produce artifacts in the upper right corner of the image during HDR fusion, which is introduced by the foreground movement of the objects in the third input LDR image. Wu's method is blurry in many contours and textures. While, the HDR image output by the C-net method can restored overall brightness of the image, many areas are mapped to the moderate brightness range, and the texture details can be seen clearly. Even in the dark area, it can still maintain good contrast, showing the changes of light, various texture details and the contour lines of objects. Therefore, our method can obtain the best result among all these methods.

4. Conclusions

In order to solve the problems of artifacts and unclear details in HDR generation algorithm of multi exposure images, a HDR generation method based on cascaded network is proposed. The effectiveness of the cascaded network are verified by quantitative and qualitative experiments. The experimental results show that the cascaded network method has strong anti-artifact ability and good image detail display effect for HDR synthesis in dynamic scene.

Acknowledgements

This work was supported in part by University of Electronic Science and Technology of China Excellent course construction project for graduate students under Grant JPKC20192-29 and Sichuan Key Laboratory of intelligent terminal under Grant SCITLAB-0015.

References

[1] Debevec P E, Malik J. "Recovering high dynamic range radiance maps from photographs", In ACM SIGGRAPH 2008 classes, pp. 31, 2008.

[2] Mertens, T., Kautz, J., Van Reeth, F. "Exposure fusion". Comput. Graph. Forum Vol.28, No. 1, pp. 382–390, 2007.

[3] Kalantari K., Ramamoorthi R. "Deep High Dynamic Range Imaging of Dynamic Scenes. ACM Trans. Graph. Vol. 36, No. 4, pp. 144:1–144:12, 2017.

[4] Wu S. Z, Xu J, Tai Y. W, Tang C.K. 2017. "Deep High Dynamic Range Imaging with Large Foreground Motions". Computer Vision- ECCV, pp. 120-135, 2018.

[5] Marnerides D., Bashford-Rogers T., Hatchett J., Debattista K. "Expandnet, a deep convolutional neural network for high dynamic range expansion from low dynamic range content". Comput. Graph. Forum, Vol. 37, No. 2, pp. 37–49, 2018.

[6] Sen P, Kalantari N K,Yaesoubi M,et al. "Robust patch-based hdr reconstruction of dynamic scenes".ACM Trans.Graph, Vol. 31, No. 6, pp. 203:1-203:11, 2012.

[7] Tursun O T, AkyuzA O, Erdem A, et al. "An objective deghosting quality metric for HDR image". Computer Graphics Forum, Vol. 35, No. 2, pp.139-152, 2016.

[8] http://empamedia.ethz.ch/hdrdatabase/index.php

[9] Narwaria M, Mantiuk R K., Silva M P D, Callet P L. "HDR-VDP-2.2: a calibrated method for objective quality prediction of high dynamic range and standard images". In Journal of Electronic Imaging, Vol. 24, No. 1, pp. 1-3, 2015.

DEEP CONVOLUTIONAL SPARSE CODING NETWORK FOR SALIENT OBJECT DETECTION IN VHR REMOTE SENSING IMAGES

XIONG XU[1], ZHOU HUANG[2], HUAIXIN CHEN[2*], BIYUAN LIU[2]

[1] Southwest China Institute of Electronic Technology, Chengdu, China
[2] School of Resources and Environment, University of Electronic Science and Technology of China, Chengdu, China
E-MAIL: *huaixinchen@uestc.edu.cn, chowhuang@std.uestc.edu.cn,

Abstract:

In order to reduce computational redundancy and increase the speed of image analysis, Saliency Object Detection (SOD) is one of the outstanding methods for Very High Resolution (VHR) remote sensing image analysis. However, Remote sensing images (RSIs) have the characteristics of diverse spatial resolutions and cluttered backgrounds, leading to the direct use of SOD methods for natural scenes generally not achieving satisfactory results. In this paper, combining the advantages of Convolutional Sparse Coding (CSC) and deep neural networks, a deep CSC network model is proposed for SOD of RSIs. First, a CSC Block (SCSB) is constructed by combining the CNN component and the Soft Shrinkage Threshold (SST) function to fully extract the effective information of the image. Then, build a multi-level coding network by stacking multiple CSCBs to enhance the perception of multi-scale and detailed information of salient targets. Finally, multi-level features are integrated in a simple way, and the entire network performs supervised learning in an end-to-end manner. The experimental results on the RSIs data set show that the proposed network model is superior to other methods in both quantitative and qualitative performance comparison.

Keywords:

Salient object detection; Convolutional sparse coding; Remote sensing image; Deep Neural Network

1. Introduction

With the continuous development of aerial photography technology, it becomes more and more easy to obtain VHR RSIs from sensors. Due to the huge amount of data and the more chaotic background compared with the natural images, it is still a great challenge to process these high spatial resolution remote sensing images efficiently. SOD aims to highlight the most attractive and visually unique targets or regions in the scene [1], and can be used as one of the effective techniques for data compression and rapid extraction of regions of interest. In remote sensing image analysis, saliency detection is applied to interest region extraction [2], area change detection [3], airport detection [4], building detection [5] and vision sensor [6] [7], etc.

Sparse representation (SR) as an advanced image analysis theoretical method is widely used in image processing and computer fields, and it has also been introduced into the SOD field. [8]. In [9], the surrounding blocks of the central image block are used to sparsely represent it, and the saliency of the image object is measured and calculated by the sparse coding length and residual error. Later, some algorithms based on background a priori [10] used superpixels or block units in the outer boundary area of the image to build a background dictionary to improve the overall saliency of the object. Recently, in [11], a background dictionary is constructed in a more compact way for sparse representation of images, so that non-saliency regions can be well distinguished.

However, traditional sparse representation methods usually use image blocks or superpixels as the basic unit of dictionary learning, but the global information of the image cannot be obtained. In addition, the dictionary training process is susceptible to hyperparameters, which leads to an increase in the cost of optimizing dictionary learning. In this article, inspired by CSC and deep neural networks, we propose a deep CSC network for SOD of RSIs. Specifically, the traditional SR is first expressed as a CSC process, and then a CSCB is constructed by combining the CNN component and the SST function, and a deep CSC network is constructed by stacking multiple CSCBs. In addition, considering the multi-scale characteristics of optical RSIs and targets, we design the backbone network as a multilayer structure. Finally, the entire proposed network is trained in an end-to-end supervised manner. The *main contributions* are summarized as follows:

(1) A multi-level CSC network for SOD of VHR RSIs. Each feature extraction layer is composed of stacked multiple CSCBs.

(2) Inspired by the mainstream feature extraction backbone network, we designed a multi-level feature extraction structure based on CSCB to adapt to the salient

objects of different scales in optical RSIs.

(3) The results of six metrics on the ORSSD [12] demonstrate that the proposed CSC network model is competitive with other methods.

2. Related works

As a special case of sparse coding, the CSC model studies the shift-invariant property of the signal, which effectively improves the signal analysis ability, so it is usually used in a variety of tasks in image processing. In [13], the paper applied the CSC model to image texture and cartoon mode separation. By using the dictionary of sample dependence, Wang *et al.* [14] proposed an online CSC model to improve the efficiency of learning large-scale samples. In the application of image super-resolution, Gu *et al.* [15]proposed a CSC scheme, whose results are better than patch-based methods.

Among the aspects of the SOD method used for RSIs, Wang *et al.* [16] introduced saliency detection to airport detection and proposed a new remote sensing image airport detection method, which improved the efficiency of target detection. Zhang *et al.* [17] proposed a novel multi-image saliency analysis model to extract regions of interest with common salient features. Recently, Huang *et al.* [18]proposed a new SOD model for optical RSIs by exploring the SR method based on learning contrast weighting atoms. Based on the shape of the network architecture, Li *et al.* [12] proposed an end-to-end network called LV-Net, which implements SOD of optical RSIs in a data-driven manner.

3. Proposed method

3.1. Principle of sparse representation

SR is a powerful and popular tool in signal analysis and processing. Usually the signal $\mathbf{x} \in \mathbf{R}^n$ divided into segments is represented by partial base atoms in the over-complete dictionary $\mathbf{D}$, that is, the signal $\mathbf{x}$ is estimated through the sparse coefficient $\boldsymbol{\alpha} \in \mathbf{R}^k$ and the dictionary $\mathbf{D}$. The calculation is as follows:

$$\mathbf{x} = \mathbf{D}\boldsymbol{\alpha} \text{ s.t. } \left\|\mathbf{x} - \mathbf{D}\boldsymbol{\alpha}\right\|_2 \le \varepsilon, \tag{1}$$

where ε is the error. The computational complexity of solving Eq. (1) increases exponentially with n. A popular strategy is to use the l_1-norm to approximate the solution (unconstrained form):

$$\arg\min_{\mathbf{D},\mathbf{A}} \frac{1}{2}\left\|\mathbf{x} - \mathbf{D}\boldsymbol{\alpha}\right\|_2^2 + \lambda\left\|\boldsymbol{\alpha}\right\|_1, \tag{2}$$

where the parameter λ represents the trade-off coefficient between the reconstruction error and the sparsity of the signal.

3.2. Convolutional sparse coding

In the CSC model, each signal segment is represented by the sum of a set of filters convolved with the corresponding code in the learning dictionary. Based on the fact that matrix multiplication operations can be replaced by convolution operations, after vectorizing $\mathbf{x}$ and α_i, The over-complete dictionary $\mathbf{D}$ is a matrix with the following transformation characteristics:

$$\begin{aligned} \mathbf{D}\alpha_i &\equiv d_i \otimes \alpha_i \\ \mathbf{D}^T\alpha_i &\equiv flipUD\left(flipLR\left(d_i\right)\right) \otimes \alpha_i, \\ &\equiv flip\left(d_i\right) \otimes \alpha_i \end{aligned} \tag{3}$$

where $\otimes$ is convolution operation. $flipUD(\,)$ and $flipLR(\,)$ follow [19], which represent the left/right and up/down flip operations of the array, respectively. A popular technique for solving the vectorized form of Eq. (2) is the Iterative Shrinkage Threshold Algorithm (ISTA) [20]:

$$\boldsymbol{\alpha}^{(k+1)} = S_{\lambda/\rho}\left(\frac{1}{\rho}\mathbf{D}^T * \left(\mathbf{x} - \mathbf{D}\boldsymbol{\alpha}^{(k)}\right) + \boldsymbol{\alpha}^{(k)}\right), \tag{4}$$

where $\rho \le \sigma_{\max}\left(\mathbf{D}^T\mathbf{D}\right)$, $\sigma_{\max}\left(x\right)$ represent the maximum eigenvalue of x. $S_\theta\left(x\right)$ is the Soft Shrinkage Threshold (SST) operator, the form can be expressed as::

$$S_\theta\left(x\right) = sign\left(x\right)\max\left(\left|x\right| - \theta, 0\right), \tag{5}$$

where $sign(\,)$ indicates the mathematical sign function. In digital image processing, assuming that the input image is $x \in \mathbf{R}^{w*h*c}$ and there are n convolution filters $f \in \mathbf{R}^{s*s*c*n}$, CSC can be modeled as follows:

$$\arg\min_m \frac{1}{2}\left\|x - f \otimes m\right\|_2^2 + \lambda R\left(m\right), \tag{6}$$

where $m \in \mathbf{R}^{h*w*n}$ refers to the sparse feature vector (or called a sparse feature map), and $R(\,)$ is the regularization function. According to Eq. (4), the update rule of the sparse feature map can be rewritten as follows:

$$m^{(i+1)} = \mathrm{Pro}x_{\lambda/\rho}\left(\frac{1}{\rho}f^T \otimes \left(\mathbf{x} - f \otimes m^{(i)}\right) + m^{(i)}\right), \tag{7}$$

where $\mathrm{Pro}x_{\lambda/\rho}(\,)$ is the proximal form of the regularization function $R(\,)$. Furthermore, Assuming $R(\,)$ is the l_1-norm, the corresponding proximal function is determined by the SST function defined by:

$$S_\theta(x) = sign(x)\,Act\left(|x| - \theta\right) \tag{8}$$

where $Act(\,)$ represents the activation function, such as the Rectified linear unit (ReLU). By the principle of algorithm unrolling [20] [21], ISTA for CSC can be constructed through neural network components. That is, the convolution filters d and d^T/ρ are replaced by two convolution layers of the decoder $DC(\,)$ and the encoder $EC(\,)$, respectively. Therefore, formula (7) can be rewritten as follows:

$$m^{(i+1)} = SST\left(BN\left(EC\left(x - DC\left(m^{(i)}\right)\right) + m^{(i)}\right)\right) \tag{9}$$

where $BN(\,)$ is batch normalization. The Eq. (9) here is called the CSCB and the stacked CSCBs can be interpreted as multi-layer representation learning, which can be regarded as an iterative automatic coding process. First, the decoder $DC(\,)$ decodes $m^{(i)}$ from the high-dimensional feature space and restores it to the image space, and then the encoder $EC(\,)$ encodes and maps the sparse residuals of the original image x and the reconstructed image from the image space to the high-dimensional feature space. Furthermore, the reconstructed residual code is added to the feature code $m^{(i)}$ of the current step. Finally, the above calculation results are updated through the normalization layer and the activation layer to obtain the input of the next cycle stage.

3.3. The proposed network structure

Considering the complexity of remote sensing scenes and the multi-scale features of salient objects, we construct a deep feature extraction network through stacked CSCBs, as shown in Fig. 1. In the encode stage, the input image first passes through layer-1 composed of two convolutional layers and one pooling layer, and then is fed to layer-2 composed of two CSCB and pooling layers. Then the feature flow passes through layer-3 and layer 4 with the same structure in sequence. Finally, two convolutional layers are passed to output the encoded features. In the decoding stage, inspired by the FCN-8s, we use the output of the last three layers of the encoding network for simple feature fusion and subsequent supervision learning.

4. Experimental results

4.1. Evaluation metrics and implementation details

In order to indicate the effect of the proposed network model, we train and test the proposed model on the public optical RSIs dataset ORSSD for SOD, which consists of 600 training images and 200 test images. Different from natural scenes, the images in the data set have a variety of spatial resolutions, the background is complex, and the target sizes vary, which is challenging.

For quantitative evaluation, we used four popular evaluation metrics, including Mean Absolute Error (MAE), S-measure (S_α), F-measure (F_β), E-measure (E_ξ) [22], Precision Recall and F-measure curves.

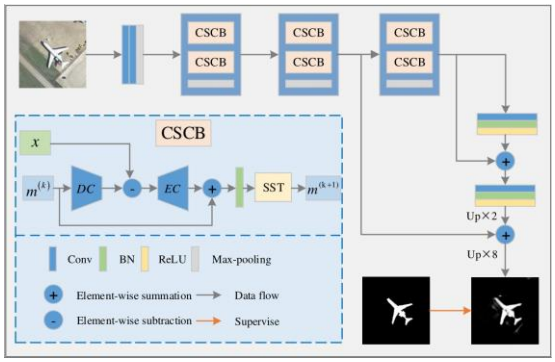


Fig.1 Proposed network architecture

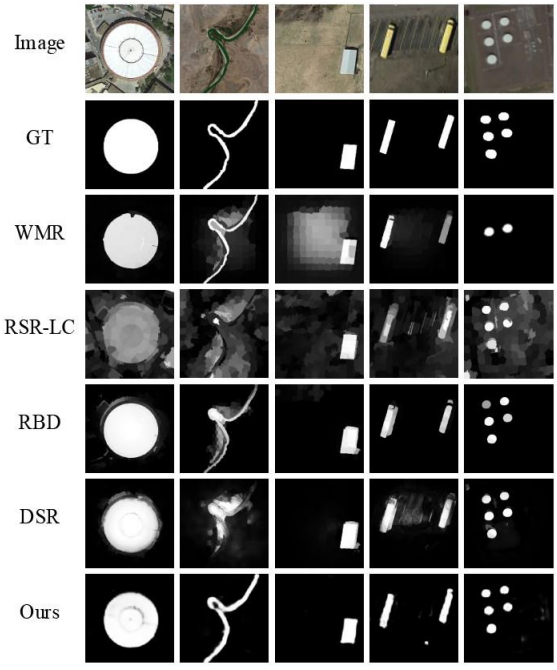


Fig.2 Visual comparisons of various methods

We use the training set and test set divided in the ORSSD data set for the training and testing phases of the model. The network model is implemented through the Pytorch toolbox, and uses inversion, cropping and multi-scale transformation operations to augment the training set. We use ADAM for network optimization, and use the binary cross-entropy loss function to train the model, and set the

maximum learning rate to 0.001.

4.2. Effectiveness comparison

We compared the proposed model with seven SOD methods, including RBD [23], LPS [24], WMR [25], DSR [26-27], SMD [27], RSR-LC [28] and RDR [29], the latter four are methods related to SR. The visual comparison is shown in Fig.2 (Due to space limitations, only four comparison methods are listed). Our method can accurately locate and highlight multi-scale salient objects. The comparison of quantitative results is shown in the Fig.3, Fig.4 and Table 1. In the comparison of various evaluation metrics, the proposed model has certain advantages.

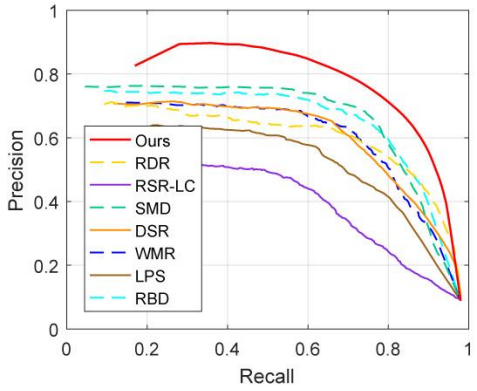


Fig.3 Comparison of PR curves

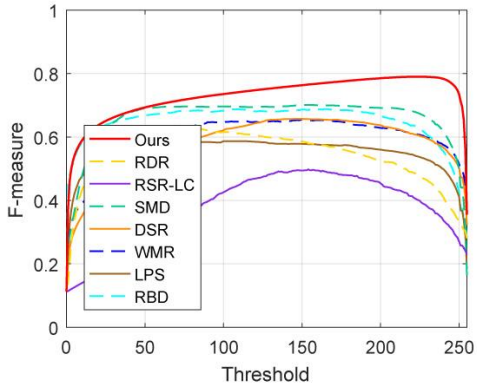


Fig.4 Comparison of F-measure curves

Table 1 Quantitative evaluations of different methods

Method	$MAE \downarrow$	$S_\alpha \uparrow$	$F_\beta \uparrow$	$E_\phi \uparrow$
RBD [23]	0.061	0.772	0.609	0.777
LPS [24]	0.088	0.694	0.497	0.705
WMR [25]	0.121	0.680	0.547	0.706
DSR [26]	0.086	0.709	0.539	0.733
SMD [27]	0.072	0.763	0.621	0.775
RSR-LC [28]	0.189	0.581	0.341	0.580
RDR [29]	0.111	0.680	0.496	0.666
Ours	**0.055**	**0.788**	**0.651**	**0.831**

Note: ↑ & ↓ denote larger and smaller is better.

5. Conclusions

Considering the advantages of sparse representation and deep convolution neural network, we propose an SOD network based on multi-level convolution sparse representation for optical RSIs, which has rich scalability. First, through theoretical analysis of CSC, the possibility of using CNN components to construct it is explained. Then stack CSCB to construct a deep network structure to perceive the multi-scale and detailed information of salient targets. Finally, integrate multiple lateral output feature streams in a simple way and train the entire network in an end-to-end manner. Various evaluation indicators on ORSSD data show that the proposed model has certain advantages. In the future, we will explore the characteristics of CSC itself and further improve the compatibility of the CSC model in DNN to achieve advanced vision task requirements.

Acknowledgements

This work is supported by the Foundation of National Key R&D Project of China (No. 2017YFC1404900) and the Foundation of Sichuan Major Science and Technology Special Project (No.2018GZDZX0017).

References

[1] Huang, Z., Chen, H. X., Zhou, T., Yang, Y. Z., & Wang, C. Y. (2020). Multi-level Cross-modal Interaction Network for RGB-D Salient Object Detection. arXiv preprint arXiv:2007.14352.

[2] Zhang L, Yue W, Li X, et al. Region-of-interest extraction based on spectrum saliency analysis and coherence-enhancing diffusion model in remote sensing images[J]. Neurocomputing, 2016, 207(C):630-644.

[3] Feng W, Sui H, Tu J, et al. A novel change detection approach based on visual saliency and random forest from multi-temporal high-resolution remote-sensing images[J]. Int. J. Remote Sens., 2018:1-24.

[4] Zhao D, Li J, Shi Z, et al. Subjective Saliency Model Driven by Multi-Cues Stimulus for Airport Detection[J]. IEEE Access, 2019, 7: 32118-32127.

[5] Li E, Xu S, Meng W, et al. Building extraction from remotely sensed images by integrating saliency cue[J]. IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens., 2016, 10(3): 906-919.
[6] Khan, Jalaluddin, et al. "SMSH: Secure Surveillance Mechanism on Smart Healthcare IoT System With Probabilistic Image Encryption." IEEE Access 8 (2020): 15747-15767.
[7] Khan, Jalaluddin et al. 'Efficient Secure Surveillance on Smart Healthcare IoT System through Cosine-transform Encryption'. 1 Jan. 2020 : 1 – 26.
[8] Y . Li, Y . Zhou, L. Xu, X. Yang, and J. Yang, "Incremental sparse saliency detection," in Proc. IEEE Int. Conf. Inf. Process., 2009, pp. 3093–3096.
[9] B. Han, H. Zhu, Y. Ding, Bottom-up saliency based on weighted sparse coding residual, Int. Conf. on Multi., 2011. pp. 1117–1120.
[10] Yi L, Qiang Z, Jungong H, et al. Salient object detection employing robust sparse representation and local consistency[J]. Image Vis Comput, 2018, 69: 155-167.
[11] Wang S, Wang M, Yang S, et al. Salient region detection via discriminative dictionary learning and joint Bayesian inference[J]. IEEE Trans. Circuits Syst. Video Technol., 2017, 28(5): 1116-1129.
[12] Li, Chongyi, et al. "Nested network with two-stream pyramid for salient object detection in optical remote sensing images." IEEE Trans. Geosci. Remote Sens. 57.11 (2019): 9156-9166.
[13] V . Papyan, Y . Romano, M. Elad, and J. Sulam, "Convolutional dictionary learning via local processing.," in Proc. IEEE Int. Conf. Comput. Vis., pp. 5306–5314, IEEE, 2017.
[14] Wang, Y., Yao, Q., Kwok, J.T. & NI, L.M.. (2018). Online Convolutional Sparse Coding with Sample-Dependent Dictionary. In Proc. Int. Conf. Mach. Learn., 80:5209-5218
[15] S. Gu, W. Zuo, Q. Xie, D. Meng, X. Feng, and L. Zhang, "Convolutional sparse coding for image super-resolution," in Proc. IEEE Int. Conf. Comput. Vis., pp. 1823–1831, IEEE, 2015.
[16] Wang, X., Lv, Q., Wang, B., & Zhang, L. (2013). Airport detection in remote sensing images: A method based on saliency map. Cognitive neurodynamics, 7(2), 143-154.
[17] Zhang, Libao, and Qiaoyue Sun. "Saliency detection and region of interest extraction based on multi-image common saliency analysis in satellite images." Neurocomputing 283 (2018): 150-165.
[18] Huang, Zhou, et al. "Detecting the Saliency of Remote Sensing Images Based on Sparse Representation of Contrast-weighted Atoms." Pattern Recog., 2020.
[19] Zhang, Menglei, Zhou Liu, and Lei Yu. "CRNet: Image Super-Resolution Using A Convolutional Sparse Coding Inspired Network." arXiv preprint arXiv:1908.01166 (2019).
[20] Karol Gregor and Yann LeCun. Learning fast approximations of sparse coding. In Proc. Int. Conf. Mach. Learn., Haifa, Israel, June 21-24, pages 399–406, 2010.
[21] Vishal Monga, Y uelong Li, and Y onina C. Eldar. Algorithm unrolling: Interpretable, efficient deep learning for signal and image processing. CoRR, abs/1912.10557, 2019.
[22] D.-P. Fan, C. Gong, Y. Cao, B. Ren, M.-M. Cheng, A. Borji, Enhanced alignment measure for binary foreground map evaluation, in: IJCAI, 2018, pp. 698–704.
[23] Zhu, Wangjiang, et al. "Saliency optimization from robust background detection." Proc. IEEE Conf. Comput. Vis. Pattern Recog., 2014.
[24] H. Li, H. Lu, Z. Lin, X. Shen, B. Price, Inner and inter label propagation: salient object detection in the wild, IEEE Trans. Image Process. 24 (10) (2015) 3176–3186.
[25] X. Zhu, C. Tang, P. Wang, H. Xu, M. Wang, J. Chen, J. Tian, Saliency detection via affinity graph learning and weighted manifold ranking, Neurocomputing 312 (2018) 239–250.
[26] X. Li, H. Lu, L. Zhang, X. Ruan, M.-H. Yang, Saliency detection via dense and sparse reconstruction, in: Proc. IEEE Int. Conf. Comput. Vis., 2013, pp. 2976–2983.
[27] H. Peng, B. Li, H. Ling, W. Hu, W. Xiong, S. J. Maybank, Salient object detection via structured matrix decomposition, IEEE Trans. Pattern Anal. Mach. Intell. 39 (4) (2016) 818–832.
[28] L. Yi, Z. Qiang, H. Jungong, W. Long, Salient object detection employing robust sparse representation and local consistency, Image Vis Comput 69 (2018) 155–167.
[29] H. Xiao, W. Ren, W. Wang, Y. Liu, M. Zhang, Salient object detection via robust dictionary representation, Multimed. Tools. Appl. 77 (3) (2018) 3317–3337.

AN EFFICIENT DEEP LEARNING MODEL FOR PREDICTING ALZHEIMER'S DISEASE DIAGNOSIS BY USING PET

PENG YIFAN[1*], DING BOWEN[23*]

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[2]CITIC-Heavy Industries Co., Ltd, Luoyang 471000, China
[3]CITIC Imaging Intelligent Technology Co., Ltd, Luoyang 471000, China
E-MAIL: yifannir@gmail.com, dingdou.cool@163.com

Abstract:

Aiming at the difficulty of artificially classifying diseased images in the field of brain positron emission tomography disease classification, we improved the network bottleneck of ResNet on this specific task in this work. And with the ensemble of improved ResNet and efficient network, our network was proposed. Also, a variety of image preprocessing methods were used to augment the characteristics of the lesion. Through experiments, the effectiveness of our proposed network structure and training strategies were proved.

Keywords:

PET image; Image preprocessing; Deep convolution network for medical; Ensemble model

1. Introduction

Brain positron emission tomography (PET) is an image that reflects the genetic, molecular, metabolic and functional status of brain diseases. It uses positron nuclides to label human metabolites (such as glucose) as an imaging agent, and reflects the metabolic changes through the uptake of the imaging agent by the lesion, thereby providing clinical biometabolic information for the disease. Parkinson's disease and Alzheimer's syndrome provide effective detection methods. Brain PET images can [1]be used to detect early Alzheimer's syndrome lesions and intervene in advance to delay the onset, which has positive significance for later rehabilitation of patients. Thus, the use of computer vision algorithms to predict PET images has important practical significance for medical aided diagnosis.

In recent years, the rank AUC of image classification tasks based on convolutional neural networks has improved in various fields. Among them, the rapid development of the model baseline is inseparable. Some scholars have applied machine learning deep networks to the prediction of Alzheimer's syndrome. Zhiguang Yang uses multi-layer convolutional neural network and PCA technology to predict AD risk [5]. It can be said that deep learning is a simple benchmark model in the prediction of AD. Taeho Jo uses multi-layer basic neural networks and convolutional neural networks, and uses neuroimaging data without preprocessing for feature selection [6]. Yiming Ding uses InceptionV3 substrate network structure for AD classification of PET images [7].

However, because the use of computer vision algorithms for the misclassification of medical image data brings great risks, the accuracy requirements for the classification of PET images are very high. And the previous scholars used a simple network structure as Substrate network, so there is more room for improvement in network structure and training strategy.

To better improve the prediction accuracy, we have proposed a stronger predictive classification model based on the efficient net substrate network for brain PET diagnosis of Alzheimer's syndrome, including more targeted image preprocessing and network model structure, training strategy adjustment, and Test Time Augmentation [10]. Then we have proved the accuracy of our algorithm by iterating different models. Through some auxiliary experiments, the effective of our proposed model also can be verified.

In the following Section 2, we describe image preprocessing, image augmentation and our network model in detail. In section 3 we introduce our training strategy, and verifies the effectiveness of our model through experiments. Finally, the paper concludes and indicate some future work in Section 4.

[1]* These authors contributed equally to this work and should be considered co-first authors

2. Model structure and training strategy

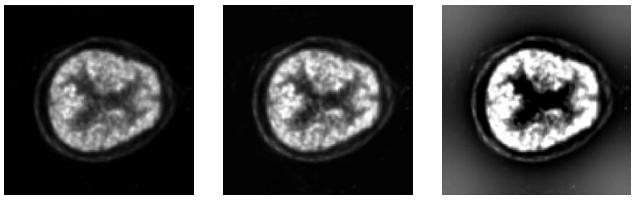
2.1. Image preprocessing and image augmentation

In the brain PET image classification task, to improve the generalization ability of the model, pre-processing of the image before training and image augmentation during training was the main methods [1].

We performed these two image preprocessing methods on the original image. The first one we called hybrid spatial augmentation, and the second one as composite augmentation.

Hybrid space augmentation: Since the dynamic range of the gray scale of the original image is very narrow and the edge of gray scale mutation is not obvious. First, Laplace transform on the image are performed to highlight the small details of the image, then increase the gray dynamic range through histogram equalization to augment the image. the original image is showed as figure 1(a), and the image obtained after mixing and augmentation is show as figure 1(b)

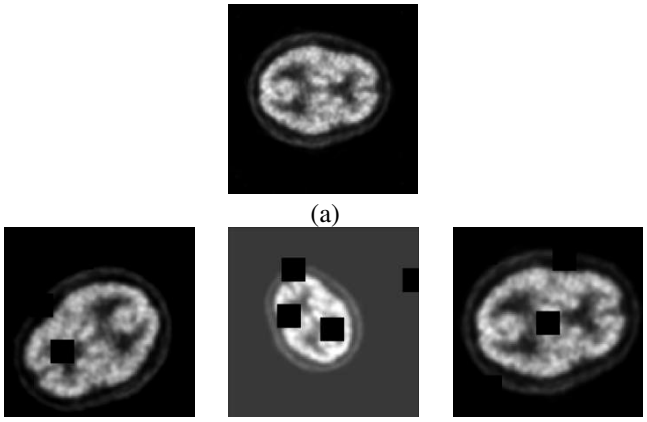
Composite augmentation: Gaussian filtering is performed on the original image, and the image is smoothed while ensuring the characteristics of feature points and feature edges. Then the filtered image and the original image are mixed and weighted to make it easier for the model to learn the lesions in the image feature. The figure 1(c) shows the image after composite augmentation.



(a) (b) (c)

Fig.1 Image preprocessing comparison. (a) is the original image, (b) is the hybrid space augmentation, (c) is the composite augmentation.

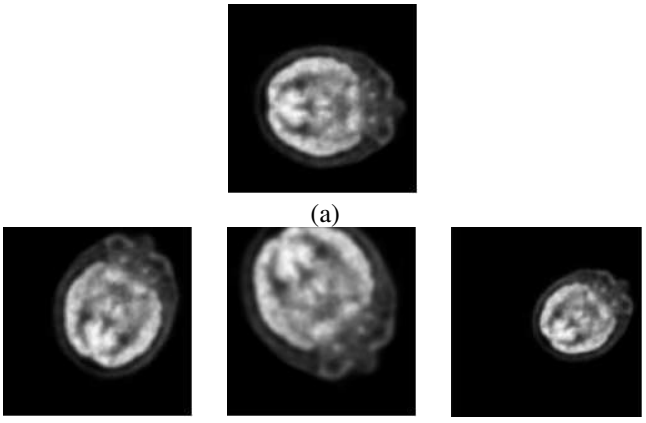
To increase the diversity of the data set, when training the model, image augmentation on the training set (including random rotation and scaling, horizontal flip, random erasure, image blur, random gamma, brightness contrast transformation, etc.) was used. At the same time, all validation set images are also subjected to a random rotation scaling transformation, and a 50% probability horizontal flip, so that the transformation method of the same image in the validation set is different in each epoch. Thereby, this method improved the generalization ability of the model. The possible augmentation effects of the same image in the training set and the validation set are shown in the figure 2 and 3.



(a)

(b) (c) (d)

Fig.2 Training data set image examples, where (a) is the original image and (b)(c)(d) is the augmented image.



(a)

(b) (c) (d)

Fig.3 Validation data set image examples, where (a) is the original image and (b)(c)(d) is the augmented image.

2.2. Model structure

In the field of machine learning, fusion of multiple different models can improve the accuracy and generalization ability. Two different net structures (ResNet based on the improved residual structure and Efficient net) constitute our model.

The first net model is based on ResNet, which changes the single convolution branch to a group convolution with 32 paths (Group Convolution), and each convolution branch is composed of a convolution kernel (1x1->3x3->1x1). After

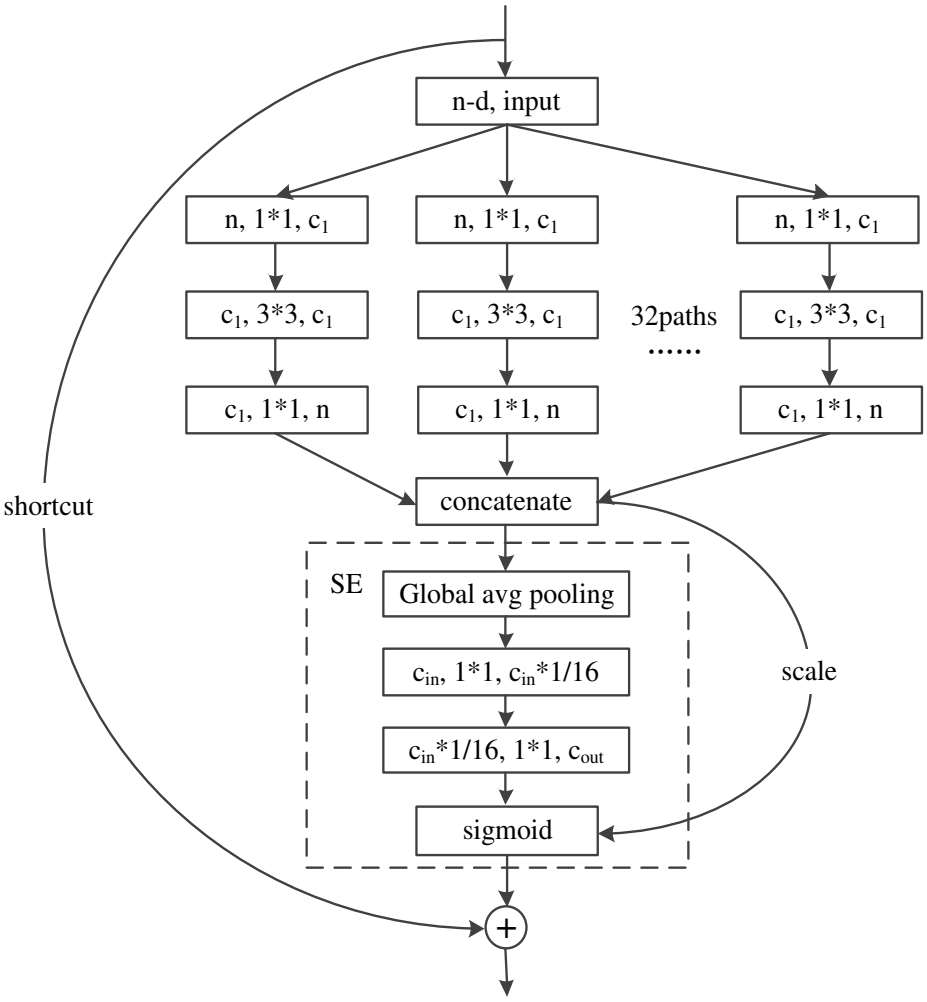


Fig.4 Improved network bottleneck

grouping convolution, each channel is spliced, and grouping convolution widens the network, making the model more expressive. At the same time, in order to improve the spatial attention of the model, the Squeeze-and-Excitation structure is embedded, which automatically acquires the importance of each feature channel through learning. Firstly, global avg pooling is applied to the obtained feature map After that, 1 x 1 convolution block is used to squeeze the image, and the output channels are converted to 1 / 16 of the input channels. Then, a 1x1 convolution block is used to extract the original channels. Finally, the weights of each channel are obtained by sigmoid and multiplied by the original feature map to focus on the most informative channel features and suppress the unimportant features. The network bottleneck is shown in the figure 4.

In order to make the model learn the global features and local features of the PET image at the same time, we changed the last pooling layer of the model to the stitching of global average pooling and global maximum pooling. On the other hand, a large number of previous studies have found that the essence of classification loss is to allocate features of different categories to hyperplanes in different feature spaces.

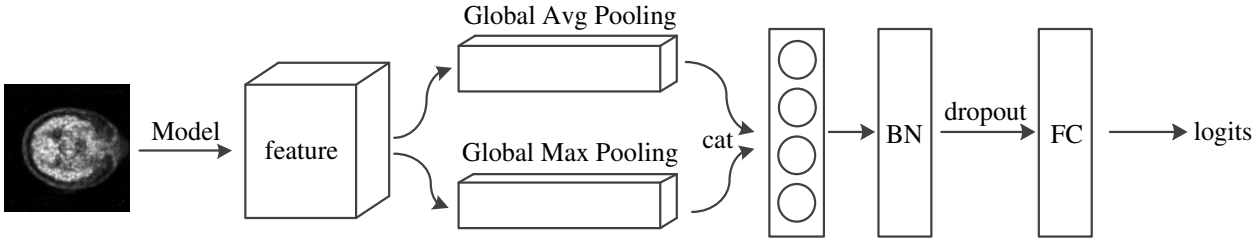


Fig.5 Network structure

According to the literature [11], the features are normalized to hyperspheres, and then the classification loss is optimized. In order to constrain the features to the hypersphere, a BN layer after the spliced pooling feature layer was added, so that the various dimensions of the feature in each batch are pulled to approximate the hypersphere distribution. Finally, dropout (0.5) is added to the fully connected layer to reduce overfitting. The network structure is shown in the figure 5.

Since the convolutional neural network can improve the accuracy of the model by increasing the depth, width, and resolution of the model, for the second model, we selected an Efficient net with variable depth and width as the first Two backbones. Due to the more complex characteristics of brain PET image lesions, a deeper network has a better classification effect on brain PET images. Finally, efficientnet-b5 based on ImageNet pre-training was selected, and dropout (0.5) was added to the fully connected layer to reduce overfitting.

2.3. Training strategy

Label smoothing. Label smoothing can improve the generalization of deep neural network [2], since our model uses binary cross entropy (BCE) as the loss function. In order to ease the constraints of hard tags on the network, the three categories of data tags are subjected to one-hot encoding with tag smoothing. On the other hand, because the data set tags can be characterized by "severity", where CN is the best, and MCI has the worst AD. For example, when the real label is CN or AD, add a label smoothing coefficient of 0.1 to the label corresponding to MCI. When the real label is MCI, set 0.05 to the other two labels. Label smoothing factor. In summary, the data set labels as follows in Table 1:

Table 1 Label smoothing rules

label coding	CN	AD	MCI
CN	0.9	0	0.1
AD	0	0.9	0.1
MCI	0.05	0.05	0.9

Top-k loss. Since each batch contains images that are easier to classify and images that are not easy to classify, the loss of each image can be large or small. In order to prevent too many simple samples from causing gradient overwhelming networks, the top 80% of each batch is selected the average loss is calculated by updating the optimizer.

Multi-scale training and model integration. The data set contains brain PET images of various sizes, (128*128), (168*168), (256*256), (336*336), (400*400). In order to adapt the model to images of various scales, to improve the robustness of the model, each model is trained with two scales (128*128, 256*256) models.

During inference, perform several image augmentations for each test image the same as the training set augmentation method (TTA). The methods include random rotation scaling and random crop scaling to change the variance distribution of the original image pixels, and pay attention to the different characteristics of each image during model inference. The augmented images are input into different models of different scales to obtain the classification probabilities and weighted average, and the final results are obtained in the form of voting for all results. The flowchart is shown in the figure 6.

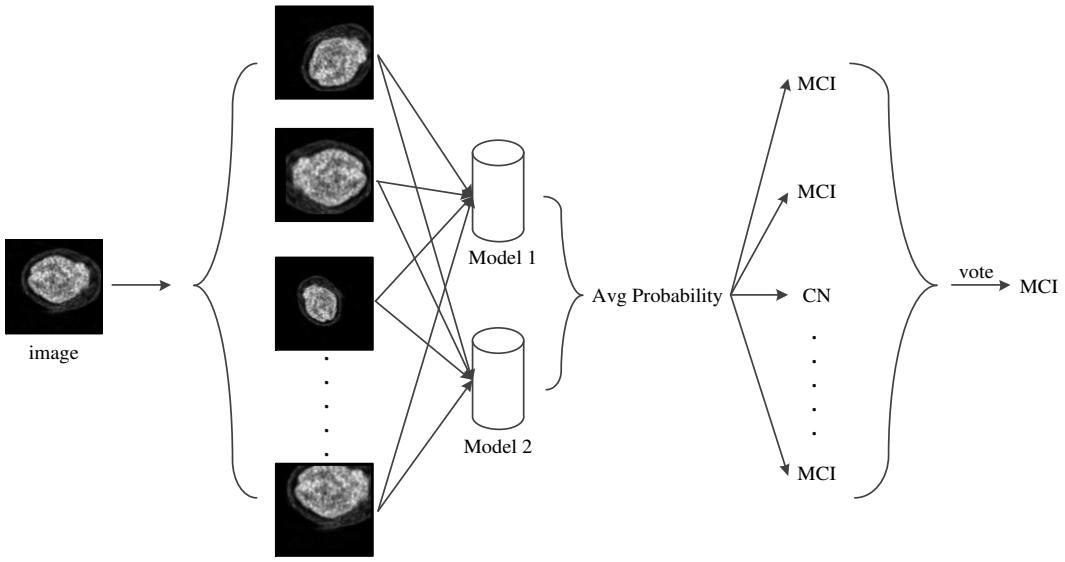


Fig.6 Model ensemble and TTA

3. Experiments

3.1. Data set and training parameters

The data used in this experiment comes from the iFlytek open platform, provided by Anhui University. The data training set contains 12000 images of three types, 4000 images of each type, 2000 images in the test set. During training, Stratified K-Fold is used to divide the training set images into training set and validation set according to the ratio of 4:1 to the labels, so that the ratio of various labels in the validation set is consistent with the training set. The training is based on the Pytorch framework, and the hardware platform is Nvidia 2080Ti. After previous experiments, the model loss decreases faster when using Adam, but the local minimum is prone to oscillations. While meeting the training speed, to ensure that the local minimum falls on the concave plane of the loss space, the model optimizer uses Amsgrad [3] At the same time, the attenuation strategy adopts cosine annealing with preheating to prevent the model from jumping out of the local minimum. The initial learning rate is 5e-4, and the periods of cosine annealing are: 14, 42. A total of 130th epochs were trained. And to improve the training speed, mixed precision training is used [9].

3.2. Evaluation Function

In this experiment, we use F1-score as the scoring metrics. As Eq 1 fellows,

$$F1 = \frac{2}{3}\left(\frac{P_1 \times R_1}{P_1 + R_1} + \frac{P_2 \times R_2}{P_2 + R_2} + \frac{P_3 \times R_3}{P_3 + R_3}\right) \quad (1)$$

In i_{th} class, where P_i, R_i is the i_{th} recall and precision of the three categories calculated by TP_i (the true value is positive, and the prediction of model considers to be positive). FP_i (the true value is negative, and the prediction of model considers to be positive). FN_i (the true value is positive, and the prediction of model considers to be negative). And P_i, R_i is calculated as fellows,

$$P_i = \frac{TP_i}{TP_i + FP_i}$$

$$R_i = \frac{TP_i}{TP_i + FN_i}$$

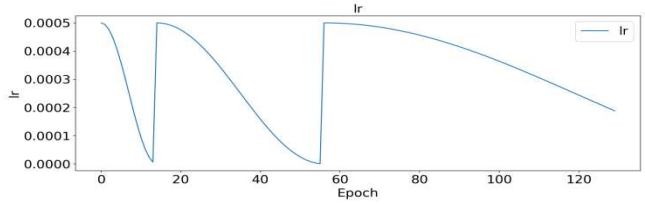
3.3. Experimental results and comparison

The differences between two preprocessing methods on PET images and the original image are compared. To eliminate the interference of other factors, Resnet-50 is chosen as the benchmark net without any augmentation during training. Table 2 shows the F1 scores of the validation set and the test set after three image preprocessing. The score of image validation set with hybrid space augmentation is higher than that of the original image, and the accuracy of composite augmentation is reduced and overfitting occurs. All subsequent images in the dataset are based on the images processed by the hybrid space augmentation.

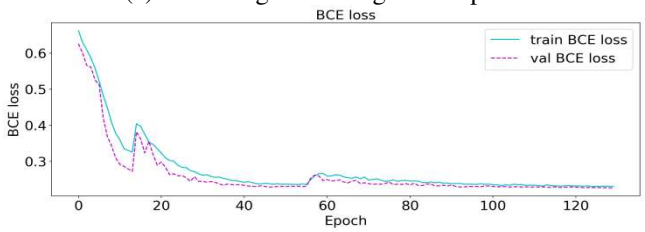
Table 2

	val	test
original image	0.881	0.865
image with hybrid space augmentation	0.889	0.875
image with composite augmentation	0.865	0.854

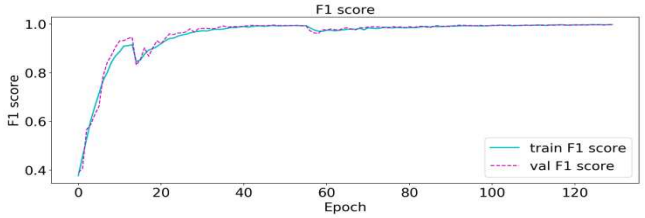
Figure 7a shows the change of learning rate when 130th epochs are trained by model efficientnet-b5, Figure 7b shows the model loss , and Figure 7c shows the evaluation index. It can be seen from the figure that whenever the learning rate warms up and the next cosine cycle starts, the model loss jumps out of the current saddle point and enters the next deeper local minimum. At the 126th epoch, the validation set has the lowest loss, which is 0.2245. At the 125th epoch, the average F1 score of the three types of validation sets is the highest, which is 0.996.



(a) learning rate change with epoch



(b) BCE loss



(c) train and val F1 score

Fig.7 Training logs

Table 3 shows the confusion matrix obtained from model 1 and model 2 and the test set after model fusion. It can be seen that efficient net (model_1) predicts MCI better, the residual network (model_2) predicts AD better with widening the network and increasing the channel attention mechanism. While after the model fusion, a higher average accuracy can be got for the predictions of CN, MCI and AD.

Table 3-1

Confusion matrix with model_1		Prediction		
		CN	AD	MCI
True	CN	581	16	3
	AD	6	583	11
	MCI	5	6	789

Table 3-2

Confusion matrix with model_2		Prediction		
		CN	AD	MCI
True	CN	586	6	8
	AD	4	591	5
	MCI	10	6	784

Table 3-3

Confusion matrix with ensemble		Prediction		
		CN	AD	MCI
True	CN	589	6	5
	AD	5	590	5
	MCI	7	4	789

On the other hand, table 4 shows the results of our comparison with other algorithms in the test set. Base in the table indicates that all the methods mentioned above are used.

Table 4

Algorithm used	F1score
model_1 with base	0.9781
model_2 with base	0.9792
two model ensemble	0.9835
efficientnet-b7 with base	0.9720
higher augmentation probability with model_1	0.9734
add center crop with base model_1	0.9799
add triplet loss with base model_1	0.9771

It can be seen from table 4 that the scores of the two models mentioned in this paper are not much different, and from Table 3, the image features of the models with different structures are not the same. The effect of fusing models with large structural differences is better than that of single model. And through many experiments, deeper model cannot improve model accuracy.

We tried a more aggressive augmentation probability (p=0.8), at this time, the training set score is reduced, and the validation set score is higher than the training set score. For we think this method adds too much noise to the training sample.

In the image augmentation method of the training set, a fixed proportion of the length and width of the center clipping is added, and then the image is resized to the acceptable length and width for the model by bilinear interpolation method. Thus, can remove a large number of useless areas of the image and improve the score of the test set. However, due to the uncertain proportion of the image lesion features, the super parameter clipping ratio still needs a lot of testing.

In the experiments of BCE loss replaced by triplet loss.

In each batch of the training set, n samples are randomly selected, and for each sample (anchor), a sample (positive and negative) is randomly sampled from the same class and different classes of images. From this, a triple is obtained and N embeddings are calculated to generate N3 triplets. For each anchor, a parameter sharing network is trained to make the cosine distance between $f(x_i^a)$ and $f(x_i^p)$ as small as possible, and the distance between $f(x_i^a)$ and $f(x_i^n)$ as far as possible. As Eq 2 shows:

$$loss = \sum_i^N \left[\left\| f(x_i^a) - f(x_i^p) \right\|_2^2 - \left\| f(x_i^a) - f(x_i^n) \right\|_2^2 + 1 \right]_+ \quad (2)$$

The F1 score of this method is slightly lower than that of base, for we think which can be caused by the possible repetition of random sampling.

4. Conclusions

We develop an efficient network based on CNN to assist people in their work. We try a variety of image preprocessing methods to augment the characteristics of the lesion. At the same time, we build two benchmark models to compare the impact of multiple image augmentations and changes in the loss function on the benchmark model. Through experiments, the most important way to judge whether brain PET images are suffering from AD is: model structure change and training strategy adjustment, image preprocessing and augmentation. On the other hand, our algorithm model has been verified on the iFLYTEK A.I. [4] developer platform, and its global third place also proved the effectiveness and practicality of our algorithm.

References

[1] Shorten C, Khoshgoftaar T M. A survey on image data augmentation for deep learning[J]. Journal of Big Data, 2019, 6(1): 60.

[2] Müller R, Kornblith S, Hinton G E. When does label smoothing. Advances in Neural Information Processing Systems. 2019: 4694-4703.

[3] Reddi S J, Kale S, Kumar S. On the convergence of adam and beyond[J]. arXiv preprint arXiv:1904.09237, 2019.

[4] http://challenge.xfyun.cn/topic/info?type=PET

[5] Yang Z, Liu Z. The risk prediction of Alzheimer's disease based on the deep learning model of brain 18F-FDG positron emission tomography[J]. Saudi Journal of Biological Sciences, 2020, 27(2): 659-665.

[6] Jo T, Nho K, Saykin A J. Deep learning in Alzheimer's disease: diagnostic classification and prognostic prediction using neuroimaging data[J]. Frontiers in aging neuroscience, 2019, 11: 220.

[7] Yang Z, Liu Z. The risk prediction of Alzheimer's disease based on the deep learning model of brain 18F-FDG positron emission tomography[J]. Saudi Journal of Biological Sciences, 2020, 27(2): 659-665.

[8] Ding Y, Sohn J H, Kawczynski M G, et al. A deep learning model to predict a diagnosis of Alzheimer disease by using 18F-FDG PET of the brain[J]. Radiology, 2019, 290(2): 456-464.

[9] Micikevicius P, Narang S, Alben J, et al. Mixed precision training[J]. arXiv preprint arXiv:1710.03740, 2017.

[10] Moshkov N, Mathe B, Kertesz-Farkas A, et al. Test-time augmentation for deep learning-based cell segmentation on microscopy images[J]. Scientific reports, 2020, 10(1): 1-7.

[11] Fan, Xing, Wei Jiang, Hao Luo, and Mengjuan Fei. "Spherereid: Deep hypersphere manifold embedding for person re-identification."Journal of Visual Communication and Image Representation (2019): 51-58.

EXTENDED SINGLE SHOOT MULTIBOX DETECTOR FOR TRAFFIC SIGNS DETECTION AND RECOGNITION IN REAL-TIME

ASSEFA ADDIS ABEBE[1], WENHONG TIAN[1,] KINGSLEY NKETIA ACHEAMPONG[1]

[1]Machine Information Intelligence Tech Lab, Information and Software Engineering, University of Electronic Science and Technology of China, Shahe Campus: No.4, Section 2, North Jianshe Road, 610054, China
E-MAIL: addi.beti@gmail.com, _wenhong@uestc.edu.cn, nketiakingsley@gmail.com

Abstract:

Real-time traffic signs detection and recognition is an essential task in autonomous driving and technology-assisted driving. In the past decades, a significant improvement in traffic sign detection and recognition has been gained due to deep learning methods. However, there is still considerable room for improvement. The traffic sign appearance variations limit the performance of the current state of the arts from perfection. Previous results have shown that the detection performance degrades for low-resolution and far scale traffic signs, resulting in high localization and recognition error and degrades CNN's object representation. Since feature maps of top layers of CNN illustrate low-level patterns that cause learning and discrimination of feature patterns challenging for the downstream recognizer. Significantly when a small-scale object passes through the layers likely to vanishes in the middle of the framework. To compensate for the loss of low-level details and localization, we proposed an Extended Single Shoot MultiBox Detector(ESSD), which integrates high resolution and easy-to-compute handcrafted feature channels with the low resolution computational expensive CNN feature channels. We apply DeepMultiBox on the hand-engineered channels (i.e., HOG+LUV and Fishers Discriminant Analysis HOG(FDA HOG) and CNN feature maps in parallel to keep a full set of object representation. We also apply color channels and shape information in a novel way to refine the localization. Experimental results on the German TSR(Trafic signs recognition) benchmark dataset shows the efficiency of the proposed approach, which is 99% mAP@0.5 IoU (intersection over union) and processes up to 60+ FPS(frames per second) in real-time and achieves recognition accuracy competitive to the state of the arts.

Keywords:

Real-Time Traffic signs detection and recognition; Autonomous driving Application; Driver Assistance Framework

1. Introduction

The intelligent traffic sign detection and recognition system (ITSDRS) is vital in realizing autonomous driving and technology-assisted driving. It involves continuous scanning and interpreting of the traffic scenes and either send a signal to a driver ahead or to take action in the case of autonomous driving. It has paramount importance for safe driving, for example, by supporting visually or cognitively distracted drivers. Hence, the response time (frames per second), object localization, the modality of features, and object representation are the critical parameters that measure the success of the ITSDRS. Several approaches have been proposed based on these parameters.

The first approach employs various combinations of hand-engineered kernels with traditional classifiers. Several powerful hand-engineered discriminating features have enhanced recognition performance and the number of frames processed per second(fps). These include the integral features channel (IFC) [1], aggregated channel feature[2], the histogram of oriented gradient HOG [3] descriptor, and SIFT [4]. The hand-engineered kernels achieved satisfactory performance with low computational complexity, but the image pyramid's paramount aspect ratio is determined by trial and error.

The second approach uses deep CNN, which shows great success in general object detection [5-6]. In this approach, different architectures have solved real-time traffic sign detection and recognition [7-8]. These architectures have improved the resolution of feature maps, recognition accuracy, and the number of frames per second. For example, class-agnostic architectures [7][9] achieve maximum recognition accuracy and robust for low resolutions and small scale objects but limited to response time. On the other hand, class-aware Frameworks [10-11] achieves the maximum number of frames per second. However, it is not suitable for low resolution and small scale objects because of the fully convolutional layers

978-0-7381-4259-3/20/$31.00 ©

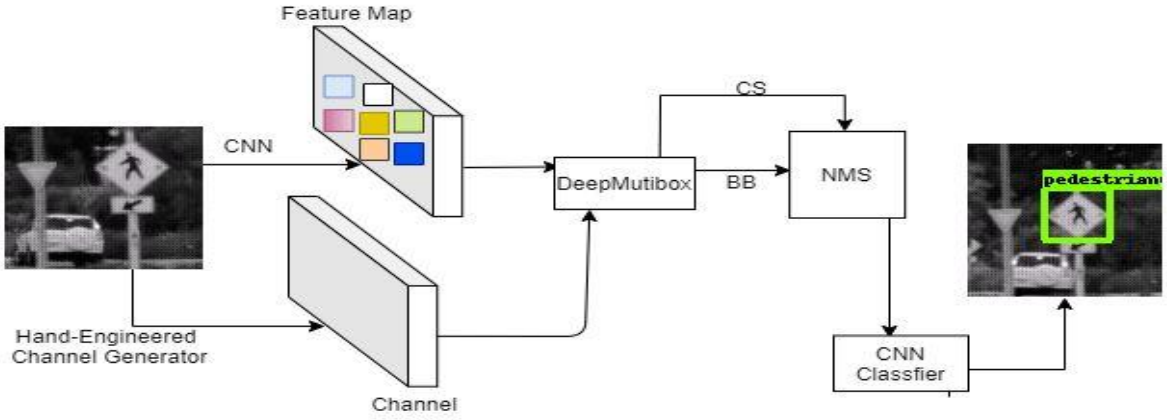


Fig.1 The General overview of FCD: The BaseNetworks generate CNN feature maps and handcrafted feature channels, and DeepMultibox generates candidate bounding boxes (BB) and Confidence score (CS), then the proposed candidate coordinate boxes and confidence score is sent to Non-Maximum Suppression (NMS) for pruning a bounding box which has a confidence score less than the threshold, finally after color and shape enhancement, is sent to ensemble CNN classifier.

That condenses the spatial size and resolution of feature maps [12].

While CNN-based approaches have consistently improved traffic signs detection and recognition performance, there is still considerable room for improvement. Performance is far from perfect, even under the most favorable condition at a comparable scale. Detection degrades catastrophically for a low-resolution traffic sign. This paper proposes a new approach called the Extended Single Shoot MultiBox Detector(ESSD) framework. Our framework overcomes the limitation associated with the two approaches above while exhibiting the positive aspects of both. It works by integrating the high resolution and easy to compute handcrafted feature channels to the low resolution and computationally inexpensive CNN feature resolution. Specifically, it extends Deep-multibox [12] combing features from the hand-engineered kernel and CNN, which results in a detailed representation of an object. The framework's detector module has various receptive fields and detailed feature maps; we also iterative refine localization error to improve IOU. Non-maximum Suppression [13] is applied to prune bounding boxes with a confidence score less than the threshold. We also propose an ensemble convolutional neural network classifier to label and group regions generated from a detector. We summarize the main contributions of this work as follows:

1) A lightweight and practical framework is proposed, which has a more generous width and can handle different scales and resolutions
2) We refine localization error for better detection performance and classification accuracy of typical traffic signs using color channels and shape information.
3) We conduct a detailed experiment and analysis; our experiment result shows 99% mAP@0.5 IoU (intersection over union) and processes up to 60+ FPS (frames per seconds) in real-time; it outperforms the art's previous state.

The remainder of this article is organized as follows. In section 2, we present a review of recent works in real-time traffic signs detection and recognition. In section 3, we discuss the proposed approach. In Section 4, Experiments and Analysis, in Section 5, we conclude and give some perspectives about future works.

2. Related Work

According to the most recent published World Health Organization (WHO) report, it was estimated that in 2018 1.35 million people were killed on the roads worldwide, as reported in road traffic injuries, a leading cause of death globally [14]. Traffic accidents are threatening the life of the public and the economy of many countries. A study [15] has proved that drivers' inability to scan and understand the road signs continuously is one reason for vehicle traffic accidents. We summarized the main approaches for real-time traffic signs recognition in the following.

A traffic-driving environment is a complex and dynamically changing scene. Factors like non-uniform

illumination, motion blur, occlusion, and hard negative samples decline a system's performance. There are mainly two approaches to tackle traffic sign detection: sliding window with image pyramids and deep learning approaches (family of R-CNN, YOLO, SSD). The sliding window-based methods commonly combine one of the handcrafted feature extractors like HOG [16], classical ViolaJones-like detector [17], integral channel feature detector [1], and Linear Discriminant Analysis (LDA) with Support Vector Machines (SVM) or Adaboost to classify traffic signs. Considering the nature of traffic signs color and rim of the plate, [18] transformed color images into gray images, then a multi-scale shape filter is performed on the gray images. An extra step is used to filter out false positives and improve precision by using SVM. These traditional approaches tend to fail in many challenging environments.

The deep learning methods integrate the base convolutional network, trained on ImageNet [19] for feature extraction. Using interest region proposal algorithms [20-21], regions of the image that potentially contain traffic signs are generated; finally, the output from ROI is recognized. There are many frameworks proposed using the family of R-CNN [22-23] using [24] classifier they achieved high accuracy. Most recently, popular detection frameworks YOLO and SSD are widely studied for generic detection tasks. Their speed is pleasing for real-time application, but their accuracy is not as good as the Family of R-CNN s. The aim is to create an efficient pedestrian detector in both fps and accuracy by inheriting both approaches' advantage.

3. Extended Single Shoot MultiBox Detector

The CNN convolution layers generate a different level of feature maps. The bottom layers feature map represents high-level features and has a low-resolution, which is used to discriminate the objects' details in an image. The top layers feature maps contain low-level features like edge patches, which are less informative and have lower resolution. While CNN feature maps of higher layers have high resolutions, the hand-engineered kernels learn (specifically the HOG+RGB)features that have a resolution close to the original image and represent detailed feature patterns. The feature maps contents are expected to have detailed features and a higher resolution scale to boost down-stream recognizers to label and categorize objects in an image effectively. Hence to achieve this, we take advantage of both sides, i.e., we integrate hand-engineered channels with CNN feature maps to construct a fused channel detector. Our proposed architecture is given in Figure.1. It consists of four cascaded modules: Firstly, features are extracted from the input image using Base CNN and a hand engineering filter in parallel. Secondly, the extracted features are sent into Deep-MutiBox, which generates bounding boxes (BB) coordinates and confidence scores (CS). Thirdly, the second step's output is sent to Non-maximum Suppression (NMS), which is used for pruning bounding boxes in which its confidence score is less than the threshold. Finally, after enhancing the color and bounding box, it is sent to the ensemble classifier to label and categorize traffic signs.

3.1. Base Convolutional Neural Network

The base network is expected to have low computational complexity and yield a detailed representation of an input image. We explore several convolutional neural network recognizers; considering the parameters mentioned above, we find that SqeezNet[30] is the most efficient framework. This framework's layer contains three tunable dimensions of the filter size; they are combined to maximize accuracy on a limited budget of parameters. The architecture's spatial size shrinks while keeping the number of filters learned relatively small compared to other network architectures.

3.2. Hand-Engineered Feature Channel

this method, precisely for traffic sign recognition, an image is first decomposed into channels. Then first-order channel features or second-order channel features are extracted using a filtered channel. Several powerful feature extraction channels have been proposed [26-27]. Of these filtered channels, we investigated the Single Bin HOG Feature (S-HOG) is the best fit for the dataset. It is an eight orientation bin; each histogram bins are responsible for the production of detailed features.

3.3. Bounding Box Generator

At this stage, both hand-engineered features and CNN feature maps are extracted. Using DeepMultibox [26], the pyramid shape structure enables it to handle different scales and resolution of objects in an image. Furthermore, this scale localization happens in a forward pass that no re-samples of feature maps are required. As a result, it makes the architecture so fast and efficient. Deep-MultiBox starts with priors. We configure our proposed framework with dense and sparse anchor boxes, and also we set each layer to have different aspect ratios. As a result,

we can handle multiple scale objects and tackle gradient vanishing caused by a small-scale object. In our case, the threshold value is set to 0.5.

3.4. Localization Refinement

When the proposed region size is less than 40 × 40, the downstream recognizer sometimes fails to label the objects. To tackle this problem, we redefine color transformation [27] since traffic signs rim and gradient information can increase the area of interest region (True positive). Each RGB pixel x is proposed to filter the image using.

$$\begin{aligned} fR(x) &= max(0, min((xR - xG), (xR - xB))) \\ fB(x) &= max(0; min(xB - xG); (xB - xB)) \\ fY(x) &= max(0; min(xR - xB); (xG - xB)) \end{aligned} \quad (1)$$

There is an intensity change at the rim of a traffic sign; thus, the image gradient improves localization. Each pixel's gradient magnitude (x,y) is calculated using an approximate formula in each resultant image.

$$\begin{aligned} \nabla I &= \left(\frac{\partial I}{\partial x}, \frac{\partial I}{\partial y} \right) \\ \left(\frac{\partial I(\mathrm{x}, \mathrm{y})}{\partial x} \right) &= \frac{I(x+1;\ y) - I(x-1;\ y)}{2} \\ \left(\frac{\partial I(\mathrm{x}, \mathrm{y})}{\partial y} \right) &= \frac{I(x;\ y+1) - I(x;\ y-1)}{2} \end{aligned} \quad (2)$$

3.5. Traffic Signs Classification

For Labelling and categorizing each traffic sign, we build a CNN recognizer, which is operationally cost-effective. This proposed architecture's kernel is split into two, the depth-wise convolution and the point-wise convolution operation. This operation can significantly reduce the computational complexity and increase feature map detail. Figure.2 shows how depth-wise convolution operates; it can save more computational cost as n grows. The framework of the ensemble classifier is resented in Table 2. it shows the full architecture of our proposed classifier. It is noted that Batch Normalization (BN) and ReLU are applied after each layer.

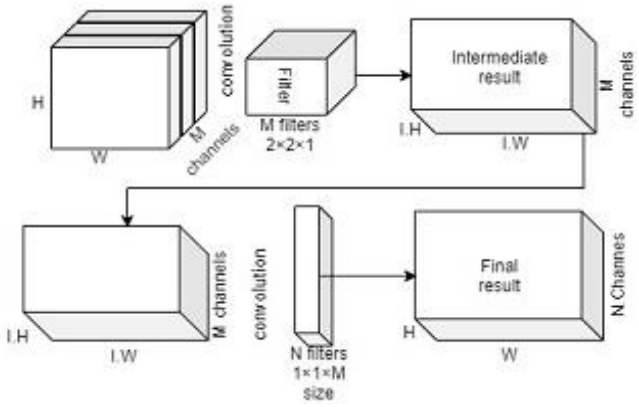


Fig.2 It shows how depthwise convolution operates.it reduces the convolution operations cost as the input size grows

4. Experiments and Analysis

The proposed architecture is trained and evaluated using the German Traffic Signs Detection Benchmark (GTSDB) dataset [21], NIVIDIA GTX 1080 GPU hardware.

4.1. Benchmark and Data Preprocessing

German TSR Benchmark (GTSRB) is used as a benchmark. Its road signs images are more challenging and representative. The dataset contains 600 training and 300 evaluation images. It has four subsets; each subset stands for a different alert, represented by a different shape and color. Each sign is a member of one of 43 class, the image scales in the dataset range from15 × 15 to 250 × 250.

4.2. The proposed Framework evaluation without Handengineered kernel features.

We have analyzed the effects of hand-engineered features on the proposed Framework; Figure.3 Shows precision and recall of the proposed framework without hand-engineered kernel features. We can observe that the precision and recall are better when hand-engineered features are integrated with CNN feature maps.

4.3. The Evaluation Extended Single Shot MultiBox Detector

Table 1 shows average mean precision (mAP) for a different combination of convolution layers with the

handcrafted feature, the spatial resolution (1 × 1) makes the worse result. The bounding boxes per class are generated then selected via non-maximum Suppression with the overlap threshold of 0.5; then, these proposals are fed into localization refinement then into the classifier.

Table 1 The mean average precision (map) of a different combination of resolution and scale of Conv layers and handcrafted features. Where N(number). BB (Bounding box)

50 × 50	27 × 27	19 × 19	13 × 13	5 × 5	1 × 1	mAP	N.BB
✓	✓	✓	✓	✓	✓	96	15862
✓	✓	✓	✓	✓		99	15858
✓	✓	✓	✓			82	15757
✓	✓	✓				62	15082
✓	✓					56	12916
✓						51	1000

We can train a very high 99% mAP@0.5 IoU after a total of 50,000 steps; the number of parameters required to build the classifier is much less than the current state of the arts. It also reduces the computational cost and accelerates the response time.

Table 2 Shows the arrangement of the proposed downstream recognizer; it has 43 class and three categories

Type/Stride	Kernel size	Input size
Conv /s1	3 × 3 × 8	32 × 32 × 3
Conv dw /s1	3 × 3 × 8	32 × 32 × 8
Conv /s1	1 × 1 × 8	32 × 32 × 8
Conv dw /s1	3 × 3 × 8	32 × 32 × 16
Conv /s2	1 × 1 × 8	32 × 32 × 8
Conv dw/s1	3 × 3 × 16	16 × 16 × 8
Conv /s1	1 × 1 × 16	16 × 16 × 16
Conv dw/s2	3 × 3 × 16	16 × 16 × 16
Conv /s1	1 × 1 × 32	8 × 8 × 16
Conv dw/s2	3 × 3 × 32	8 × 8 × 32
Dense	/	4 × 4 × 32
Dropout	/	(*None;* 512)
Batch Normalization	/	(*None;* 128)
Dropout	/	(*None;* 128)
Dense	/	(*None;* 43)
Activation	/	(*None;* 43)

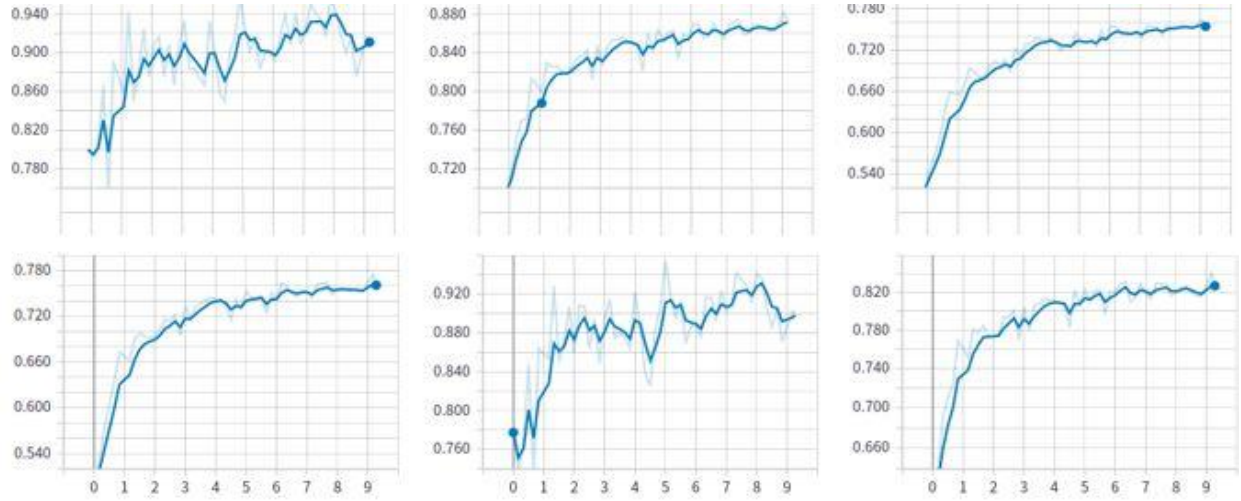


Fig.3 The handcrafted feature's effect on traffic sing detection performance; the top row figure shows the proposed framework's precision without a hand-engineered feature. The bottom row shows using an integration of both features.

(a)

(b)

Fig.4 The above figure shows a sample detection output of the proposed framework. The outcomes show that our detector is very vigorous and effectively detect (a,b)

5. Conclusion

In this paper, A straightforward and lightweight framework is proposed for detecting traffic signs in real-time. The deep convolutional neural network and hand-engineered kernel are combined in a novel way to get a detailed representation of an object. Every feature map cell is associated with different bounding boxes of various dimensions and aspect ratios; thus, multiple scales and resolutions can be handled. Moreover, it can detect beyond the limitations of colors and shapes. Finally, candidate bounding boxes are categorized using an efficient classifier. We plan to integrate this framework

Acknowledgments

This research is sponsored by the National Key Research and Development Plan and Award. Grant number:2018AAA0103203

References

[1] Piotr Dollar, Zhuowen Tu, Pietro Perona, and Serge Belongie. Integral ´channel features. 2009

[2] Ankit Verma, Ramya Hebbalaguppe, Lovekesh Vig, Swagat Kumar, andEhtesham Hassan. Pedestrian detection via mixture of cnn experts and thresholded aggregated channel features. In Proceedings of the IEEE International Conference on Computer Vision Workshops, pages 163–171, 2015. Tony Lindeberg. Scale invariant feature transform. 2012.

[3] Navneet Dalal and Bill Triggs. Histograms of oriented gradients
for human detection. In 2005 IEEE computer society conference on computer vision and pattern recognition (CVPR'05), volume 1, pages 886–893. IEEE, 2005. Wei Liu, Dragomir Anguelov, Dumitru Erhan, Christian Szegedy, Scott Reed, Cheng-Yang Fu, and Alexander C Berg. Ssd: Single shot multibox detector. In European conference on computer vision, pages 21–37. Springer,

[4] Tony Lindeberg. Scale invariant feature transform. 2012.

[5] Shaoqing Ren, Kaiming He, Ross Girshick, and Jian Sun. Faster r-cnn: Towards real-time object detection with region proposal networks. In Advances in neural information processing systems, pages 91–99, 2015.

[6] Wei Liu, Dragomir Anguelov, Dumitru Erhan, Christian Szegedy, Scott Reed, Cheng-Yang Fu, and Alexander C Berg. Ssd: Single shot multibox detector. In European conference on computer vision, pages 21–37. Springer, 2016. Transportation Systems, 18(12):3290–3302, 2017.

[7] Jia Li and Zengfu Wang. Real-time traffic sign recognition based on efficient cnns in the wild. IEEE Transactions on Intelligent Transportation Systems, 20(3):975–984, 2018 Hengliang Luo, Yi Yang, Bei Tong, Fuchao Wu, and Bin Fan. Traffic sign recognition using a multi-task convolutional neural network. IEEE Transactions on Intelligent Transportation Systems, 19(4):1100–1111,2017.

[8] Dongdong Wang, Xinwen Hou, Jiawei Xu, Shigang Yue, and ChengLin Liu. Traffic sign detection using a cascade method with fast feature extraction and

saliency test. IEEE Transactions on Intelligent Transportation Systems, 18(12):3290–3302, 2017 Yiqiang Wu, Zhiyong Li, Ying Chen, Ke Nai, and Jin Yuan. Real-time traffic sign detection and classification towards real traffic scene. Multimedia Tools and Applications, pages 1–19, 2020.

[9] Yizhi Song, Ruochen Fan, Sharon Huang, Zhe Zhu, and Ruofeng Tong. A three-stage real-time detector for traffic signs in large panoramas. Computational Visual Media, 5(4):403–416, 2019

[10] Shu-fang ZHANG and Tong ZHU. Traffic sign detection and recognition based on residual single shot multibox detector model. Journal of ZheJiang University (Engineering Science), 53(5):940–949, 2019. Zhigang Liu, Juan Du, Feng Tian, and Jiazheng Wen. Mr-cnn: A multi-scale region-based convolutional neural network for small traffic sign recognition. IEEE Access, 7:57120–57128, 2019.

[11] NS Artamonov and PY Yakimov. Towards real-time traffic sign
recognition via yolo on a mobile gpu. In Journal of Physics: Conference Series, volume 1096, 2018. Alexander Neubeck and Luc Van Gool. Efficient non-maximum Suppression. In 18th International Conference on Pattern Recognition (ICPR'06), volume 3, pages 850–855. IEEE, 2006.

[12] Zhaowei Cai, Quanfu Fan, Rogerio S Feris, and Nuno Vasconcelos. A unified multi-scale deep convolutional neural network for fast object detection. In European conference on computer vision, pages 354–370.
Springer, 2016.

[13] Alexander Neubeck and Luc Van Gool. Efficient non-maximum suppression. In 18th International Conference on Pattern Recognition (ICPR'06), volume 3, pages 850–855. IEEE, 2006.

[14] World Health Organization et al. Global status report on road safety 2018:

[15] Addis Abebe Assefa and Tian Wenhong. Bio-mechanical distracted driver recognition based on stacked autoencoder and convolutional neural network. In 2019 IEEE 2nd International Conference on Information Communication and Signal Processing (ICICSP), pages 449–453. IEEE, 2019

[16] Sebastian Houben, Johannes Stallkamp, Jan Salmen, Marc Schlipsing, and Christian Igel. Detection of traffic signs in real-world images: The german traffic sign detection benchmark. In The 2013 international joint conference on neural networks (IJCNN), pages 1–8. IEEE, 2013.

[17] Cristian Lorenz, I-C Carlsen, Thorsten M Buzug, Carola Fassnacht, and Jurgen Weese. A multi-scale line filter with automatic scale selectionbased on the hessian matrix for medical image segmentation. In International Conference on Scale-Space Theories in Computer Vision,

[18] Yihui Wu, Yulong Liu, Jianmin Li, Huaping Liu, and Xiaolin Hu. Traffic sign detection based on convolutional neural networks. In The 2013international joint conference on neural networks (IJCNN), pages 1–7.

[19] Jia Deng, Wei Dong, Richard Socher, Li-Jia Li, Kai Li, and Li FeiFei. Imagenet: A large-scale hierarchical image database. In 2009 IEEE conference on computer vision and pattern recognition, pages 248–255.

[20] Jasper RR Uijlings, Koen EA Van De Sande, Theo Gevers, and
Arnold WM Smeulders. Selective search for object recognition. International journal of computer vision, 104(2):154–171, 2013.

[21] Christian Szegedy, Scott Reed, Dumitru Erhan, Dragomir Anguelov, and Sergey Ioffe. Scalable, high-quality object detection. arXiv preprint arXiv:1412.1441, 2014

[22] Evan Peng, Feng Chen, and Xinkai Song. Traffic sign detection with convolutional neural networks. In International Conference on Cognitive Systems and Signal Processing, pages 214–224. Springer, 2016.

[23] Samuele Salti, Alioscia Petrelli, Federico Tombari, Nicola Fioraio, and Luigi Di Stefano. A traffic sign detection pipeline based on interest region extraction. In The 2013 International Joint Conference on Neural Networks (IJCNN), pages 1–7. IEEE, 2013

[24] Huizi Mao, Song Yao, Tianqi Tang, Boxun Li, Jun Yao, and Yu Wang. Towards real-time object detection on embedded systems. IEEE Transactions on Emerging Topics in Computing, 6(3):417–431, 2016.

[25] Forrest N Iandola, Song Han, Matthew W Moskewicz, Khalid Ashraf, William J Dally, and Kurt Keutzer. Squeezenet: Alexnet-level accuracy with 50x fewer parameters and¡ 0.5 mb model size. arXiv preprint arXiv:1602.07360, 2016.

[26] Niklas Pettersson, Lars Petersson, and Lars Andersson. The histogram feature-a resource-efficient weak classifier. In 2008 IEEE Intelligent Vehicles Symposium, pages 678–683. IEEE, 2008

[27] Gary Overett and Lars Petersson. Large scale sign detection using hog feature variants. In 2011 IEEE Intelligent Vehicles Symposium (IV).

A TENSOR MODELING FOR VIDEO RAIN STREAKS REMOVAL APPROACH BASED ON THE MAIN DIRECTION OF RAIN STREAKS

DOU YAPING[1], ZHANG PING[1], ZHOU YING[1], ZHANG LINGYI[1]

[1]School of Optoelectronics Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610051, China
E-MAIL: 17780547267@163.com, pingzh@uestc.edu.cn

Abstract:

The algorithms for video rain streaks removal do not properly consider the influence of wind on the main direction of rain streaks. They do not rotate or only perform a rough rotation when rain streaks deviate from the vertical direction, resulting in residual rain patterns or blurred background. Therefore, a sparse tensor model based on the main direction of rain streaks is suggested for video rain streaks removal in this paper. First, the first-order directional derivative (FODD) filter is used to obtain the rain image with the best background suppression effect. Second, we calculate its histogram of oriented gradient (HOG) feature to match the rain streaks image library. The main direction of rain streaks and the rotation angle of the global model are determined by the matching result. Finally, a sparse tensor is constructed with a rotation-angle based regularization term for rain streaks removal. In addition, the tensor nuclear norm (TNN) is replaced with the tensor truncated nuclear norm (T-TNN) to ensure the global low rank of the rain free video. The alternating direction method of multipliers (ADMM) is used to work out the model. The experimental results represent the excellence of the proposed method compared with the baseline methods in terms of the value of peak signal-to-noise ratio (PSNR) and the value of structural similarity (SSIM).

Keywords:

Video rain streaks removal; FODD; Sparse tensor; Sparse regularization; Tensor truncated nuclear norm

1. Introduction

The algorithms of video rain streaks removal can be split into three categories: rain streaks removal algorithm based on dictionary-learning and sparse-coding, rain streaks removal algorithm based on model and rain streaks removal algorithm based on deep learning. The first sort, Kang et al. [1] divided an image into two parts which are the high and the low frequency parts. And then he get the rain streaks from the high one part. Rain streaks removal algorithm based on model, Chen et al. [2] constrained the rain streaks through the total variation regular term to realize the separation of rain streaks. Rain streaks removal algorithm based on deep learning, Zhang et al. [3] suggested a convolutional neural network based on density perception.

Based on the research of Jiang [4], we propose a sparse tensor model based on the main direction of rain streaks. The main innovations: 1. Determine the main direction of rain streaks 2. The T-TNN is used to replace the TNN.

It consists of the following parts: Section 2 shows the proposed model. Section 3 describes the results of experiment. Section 4 shows the conclusions of the paper.

2. The proposed model

2.1. The main direction of rain streaks

We use FODD to process the image to get filter images which have 8 directions in Figure 2. The angels are [0° ,90°,45°,135°,180°,270°,225°,315°].

Choosing the best filter image which background is suppressed in a good effect. We calculate its HOG feature to match the rain streaks image library. We set 10° as a gradient difference and get a set with 9 directions [50°,60°,70°,80°,90°,100°,110°,120°,130°] as the rain image library . Finally, we obtain the corresponding angel of the main direction of rain streaks, which is recorded as $\tilde{\alpha}$. The angel which the image needs to be rotated is recorded as α. When $\tilde{\alpha}$ is less than 90°, the rainy image as input to the model which needs to be rotated counterclockwise by 90°-$\tilde{\alpha}$, otherwise rotated by $\tilde{\alpha}$-90° clockwise.

$$\alpha = \begin{cases} 90° - \tilde{\alpha} & (\tilde{\alpha} \le 90°) \\ \tilde{\alpha} - 90° & (\tilde{\alpha} > 90°) \end{cases} \quad (1)$$

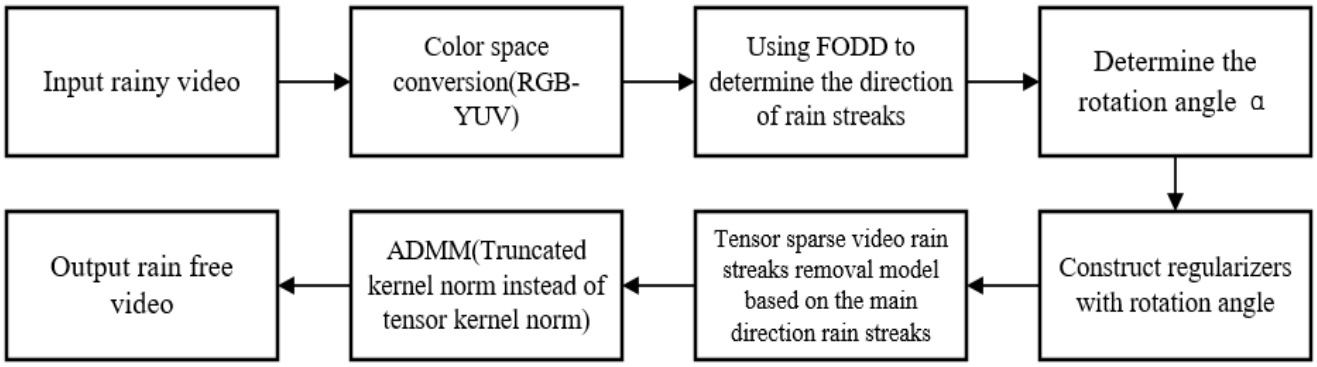


Fig.1 The framework of our method

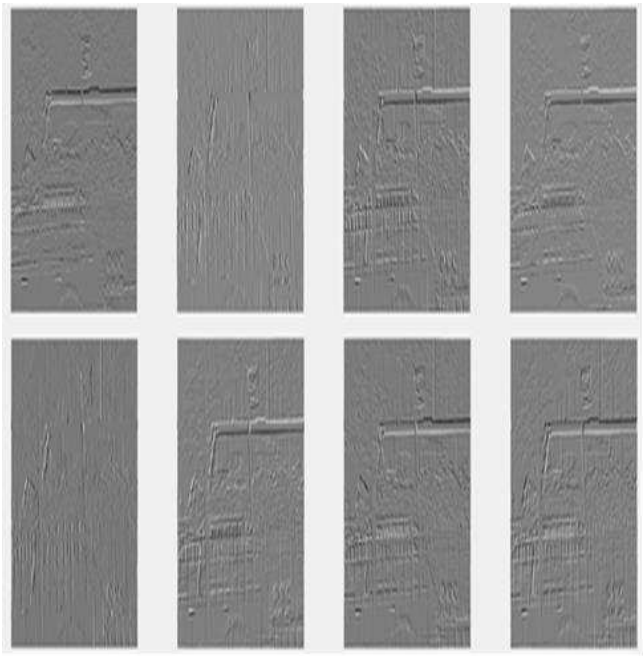


Fig.2 The result of using FODD to process rainy image. From top to bottom，from left to right: the angels are [0° ,90°,45°,135°,180°,270°,225°,315°].

2.2. The proposed model

The rainy image needs to be rotated by α, record it as D_θ. $\|D_\theta\mathcal{R}\|_1$ is used to enhance the sparsity of rain streaks and $\|\nabla_y(D_\theta\mathcal{R})\|_1$ is used to firm the smoothness of rain streaks along y which is the vertical direction. And then, $\|\nabla_y(D_\theta\mathcal{B})\|_1$ and $\|\nabla_t(D_\theta\mathcal{B})\|_1$ is used to boost the smoothness of the rain free video along the horizontal direction and along the time direction, respectively. The T-TNN is used to instead the TNN. The T-TNN $\mathcal{B} \in R^{m*n*t}$ is defined as:

$$||\mathcal{B}||_r = ||\bar{\mathcal{B}}^{(1)}||_* - \max_{\substack{\mathcal{G}\mathcal{G}^T=I \\ \mathcal{H}\mathcal{H}^T=I}} tr(\mathcal{G}*\mathcal{B}*\mathcal{H}^T) \quad (2)$$

$$\mathcal{G} = \mathcal{U}(:,1:\mathrm{r},:)^{\mathrm{T}}, \mathrm{H} = \mathcal{V}(:,1:\mathrm{r},:)^{\mathrm{T}} \quad (3)$$

Where $\mathcal{B} = \mathcal{U}*\mathcal{S}*\mathcal{V}^T$, $\mathcal{G}$, $\mathcal{H}$ are intercepted from $\mathcal{U}$, $\mathcal{V}$.

The model can be succinctly formulated as:

$$\begin{aligned}\arg\min_{B,R} \alpha_1\|\nabla_y(D_\theta\mathcal{R})\|_1 + \alpha_2\|D_\theta\mathcal{R}\|_1 + \alpha_3\|\nabla_x(D_\theta\mathcal{B})\|_1 \\ + \alpha_4\|\nabla_t(D_\theta\mathcal{B})\|_1 \\ + rank(D_\theta\mathcal{B}) \quad (4)\end{aligned}$$

$$\text{s.t}\ \ \mathcal{O} = \mathcal{B} + \mathcal{R} \qquad \mathcal{O},\mathcal{B},\mathcal{R} \in \mathbb{R}^{m*n*t} \geq 0$$

Where $\mathcal{O}$，$\mathcal{B}$，$\mathcal{R}$ are the tensor which is the three dimensional, suggesting rainy video, rain free video and rain streaks, respectively. Where ∇_x, ∇_y and ∇_t are the derivative operators of the vertical, the horizontal and the time direction, respectively.

The above model uses the ADMM to solve the problem:

$$\begin{aligned}\arg\min_{\mathcal{Y},\mathcal{S},\mathcal{X},\mathcal{T},\mathcal{R}} \alpha_1\big||\mathcal{Y}|\big|_1 + \alpha_2\big||\mathcal{S}|\big|_1 + \alpha_2\big||\mathcal{X}|\big|_1 + \alpha_4\big||\mathcal{T}|\big|_1 \\ + ||\mathcal{L}||_* \\ - tr(\mathcal{G}*\mathcal{L}*\mathcal{H}^T) \quad (5)\end{aligned}$$

$$\text{s.t}\ \mathcal{Y} = \nabla_y(D_\theta\mathcal{R}), \mathcal{S} = D_\theta\mathcal{R}, \mathcal{X} = \nabla_x(D_\theta(\mathcal{O}-\mathcal{R}))$$

$$\mathcal{T} = \nabla_t\big(D_\theta(\mathcal{O}-\mathcal{R})\big), \qquad \mathcal{L} = D_\theta\mathcal{O} - D_\theta\mathcal{R}$$

Where $D_\theta(\mathcal{O}-\mathcal{R}), D_\theta\mathcal{R}$ and $D_\theta\mathcal{O}$ recorded as $\mathcal{O}_{D_\theta} -$

$\mathcal{R}_{D_\theta}, \mathcal{R}_{D_\theta}$ *and* $\mathcal{O}_{D_\theta}$.

1) $\mathcal{R}_{D_\theta}$-sub-problem:

$$\mathcal{R}_{D_\theta}{}^{(t+1)} = \mathcal{F}^{-1}\left(\frac{\mathcal{F}(\mathcal{M}_1)}{\mathcal{F}(\mathcal{M}_2)}\right) \quad (6)$$

Where $\mathcal{F}$ suggests the fast Fourier transform (FFT) and $\mathcal{F}^{-1}$ expresses the converse of FFT.

2) $\mathcal{Y}$,$\mathcal{S}$,$\mathcal{X}$ and $\mathcal{T}$ -sub-problem:

$$\mathcal{Y}^{(t+1)} = soft_{\frac{\alpha_1}{\beta}}\left(\nabla_y \mathcal{R}_{D_\theta}{}^{(t)} + \frac{\Lambda_1{}^{(t)}}{\beta_1}\right) \quad (7)$$

$$\mathcal{S}^{(t+1)} = soft_{\frac{\alpha_2}{\beta}}(\mathcal{R}_{D_\theta}{}^{(t)} + \frac{\Lambda_2{}^{(t)}}{\beta_2}) \quad (8)$$

$$\mathcal{X}^{(t+1)} = soft_{\frac{\alpha_3}{\beta}}\left(\nabla_x\left(\mathcal{O}_{D_\theta} - \mathcal{R}_{D_\theta}{}^{(t)}\right) + \frac{\Lambda_3{}^{(t)}}{\beta_3}\right) \quad (9)$$

$$\mathcal{T}^{(t+1)} = soft_{\frac{\alpha_4}{\beta}}(\nabla_t(\mathcal{O}_{D_\theta} - \mathcal{R}_{D_\theta}{}^{(t)}) + \frac{\Lambda_4{}^{(t)}}{\beta_4}) \quad (10)$$

Where $soft_{\frac{\alpha}{\beta}}(\mathcal{Y}) = sign(\mathcal{Y})\max(|\mathcal{Y}| - \frac{\alpha}{\beta}, 0)$.

3) $\mathcal{L}$ -sub-problem:

$$\mathcal{L}^{(t+1)} = \sum_{i=1}^{3} \frac{1}{3} fold_i\left(A_i^{(t+1)}\right) - tr(\mathcal{G} * \mathcal{L} * \mathcal{H}^T) \quad (11)$$

Where $A_i^{(t+1)} = \mathcal{D}_{\frac{1}{\beta_5}}(\mathcal{B}_{D_\theta}{}_{(i)}^{(t)} + \frac{\Lambda_5{}_{(i)}^{(t)}}{\beta_5})$, $\mathcal{D}_{\frac{1}{\beta_5}}(M)$ means that the value of M after the operation of soft thresholding.

4) Multipliers updating:

$$\Lambda_1^{(t+1)} = \Lambda_1^{(t)} + \beta_1(-\mathcal{Y}^{(t+1)} + \nabla_y(\mathcal{O}_{D_\theta} - \mathcal{R}_{D_\theta}{}^{(t+1)}))$$

$$\Lambda_2^{(t+1)} = \Lambda_2^{(t)} + \beta_2(-\mathcal{S}^{(t+1)} + (\mathcal{O}_{D_\theta} - \mathcal{R}_{D_\theta}{}^{(t+1)}))$$

$$\Lambda_3^{(t+1)} = \Lambda_3^{(t)} + \beta_3(-\mathcal{X}^{(t+1)} + \nabla_x(\mathcal{R}_{D_\theta}{}^{(t+1)})) \quad (12)$$

$$\Lambda_4^{(t+1)} = \Lambda_4^{(t)} + \beta_4(-\mathcal{T}^{(t+1)} + \nabla_t(\mathcal{R}_{D_\theta}{}^{(t+1)}))$$

$$\Lambda_5^{(t+1)} = \Lambda_5^{(t)} + \beta_5\left(\mathcal{R}_{D_\theta}{}^{(t+1)} - \mathcal{L}^{(t+1)}\right)$$

Where $\Lambda = [\Lambda_1, \Lambda_2, \Lambda_3, \Lambda_4, \Lambda_5]$ is the Multipliers of the Lagrange and $\beta = [\beta_1, \beta_2, \beta_3, \beta_4, \beta_5]$ are is a positive penalty parameter.

Alg.1 Algorithm of the paper proposed method

Input: The rainy video: $\mathcal{O}_{D_\theta}$

1. Initialization: $\mathcal{R}^{(0)} = zeros(m * n * t)$, $\mathcal{B}^{(0)} = \mathcal{O}$
2. While not converged do
3. Update $\mathcal{R}$ via (6);
4. Update $\mathcal{Y}, \mathcal{S}, \mathcal{X}$ and $\mathcal{T}$ via (7~10);
5. Update $\mathcal{L}$ via (11);
6. Update multipliers via (12);
7. End while

Output: rain streaks: $\mathcal{R}$ and rain free video: $\mathcal{B} = \mathcal{O} - \mathcal{R}$

3. Experimental results

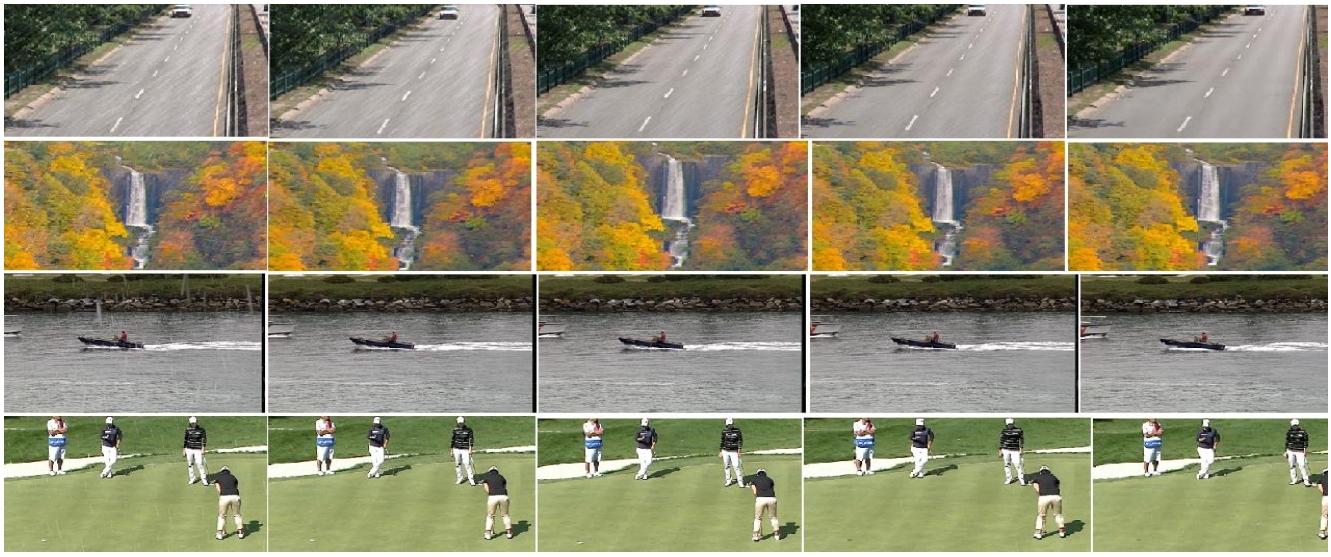
We compare our method with temporal correlation and low-rank matrix completion method (LRM) [5] and discriminatively intrinsic priors method (DIP) [4].

We observe from Table 1 that our method is superior to the other two methods when the rain streaks deviate from the vertical direction more than 15°, such as the "highway" (right 45°) and "fall" (right 30°) videos. Moreover the performance of our method is enhanced with the increase of the deviation angle of the rain streaks. When the deviation angle is less than 15°, it shows that our method and DIP method have similar effects in removing rain streaks, and they are both superior to the LRM method.

Figure 3 shows, the above three methods have little difference in the effect of removing rain streaks when the deviation angle is less than 15°. However, our method removes the rain streaks largely and keeps the particulars of the image when the angle is more than 15°. But the other two methods still retain many rain streaks

4. Conclusions

When rain streaks deviate from the vertical direction, we suggest a sparse tensor video rain streaks removal model based on the main direction of rain streaks. The results of our experimental show that this method can effectively remove rain streaks while retaining the the particulars of the image background to a greater extent, and the values of PSNR and SSIM are relatively high.



The frames of rainy image LRM DIP The proposed method The clean image

Fig.3 The results of rain streak removal. From top to bottom: the "highway", "fall", "coast" and "golf", respectively.

Table 1 The results of rain streaks removal

Raniy video	method	PSNR/dB	SSIM
highway (right 45°)	LRMC	28.412	0.811
	DIP	34.197	0.925
	Proposed	34.675	0.934
fall (right 30°)	LRMC	33.314	0.726
	DIP	34.197	0.897
	Proposed	35.141	0.9111
cost (0°)	LRMC	28.741	0.911
	DIP	31.889	0.961
	Proposed	32.747	0.952
golf (left 15°)	LRMC	33.198	0.915
	DIP	33.742	0.819
	Proposed	33.691	0.937

Acknowledgements

This research is supported by National Natural Science Foundation of China (No. 62075031) and the Science and Technology Planning Project of Sichuan Province, China (No.2019YFG0307) and the Partially funded by Intelligent Terminal Key Laboratory of SiChuan Province Open Project Grant (No. SCITLAB-0016 and SCITLAB-0009).

References

[1] L.-W. Kang, C.-W. Lin, Y.-H. Fu. Automatic Single-image-based Rain Streaks Removal Via Image Decomposition[J]. IEEE Transactions on Image Processing, 2012, 21: 1742–1755

[2] Y.-L. Chen, C.-T. Hsu. A generalized low-rank appearance model for spatio-temporally correlated rain streaks[C]. Proceedings of the IEEE International Conference on Computer Vision Darling, Harbour, Sydney, Australia, 2013, 1968–1975

[3] H. Zhang, V.-M. Patel. Density-Aware Single Image De-Raining Using a Multi-Stream Dense Network[C]. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018,695–704

[4] T.-X. Jiang, T.-Z. Huang, X.-L. Zhao, et al. A Novel Tensor-based Video Rain Streaks Removal Approach via Utilizing Discriminatively Intrinsic Priors[C]. IEEE Computer Vision and Pattern Recognition (CVPR), 2017, 4057–4066

[5] J.-H. Kim, J.-Y. Sim, C.-S. Kim, Video deraining and desnowing using temporal correlation and low-rank matrix completion, IEEE Trans. Image Process. 24 (2015) ,2658–267

VEHICLE TO EVERYTHING (V2X) COMMUNICATION PROTOCOL BY USING VEHICULAR AD-HOC NETWORK

MUHAMMAD AHTSAM NAEEM[1], XIAOLIN JIA[1], MUHAMMAD ASIM SALEEM[2],WASIF AKBAR[3], AFZAAL HUSSAIN[4], SHAHBAZ NAZIR[4], KHWAJA MUTAHIR AHMAD[2]

[1] School of Computer Science and Technology, Southwest University of Sciences and Technology, China
[2] School of Information and Software Engineering, University of Electronic Sciences and Technology of China (UESTC)
[3] School of Computer Science and Engineering, University of Electronic Sciences and Technology of China (UESTC)
[4] Department of Information Technology, Government College University, Faisalabad, Pakistan
E-MAIL: muhammadahtsam1@outlook.com, my_jiaxl@163.com, asim.saleem1@hotmail.com, sewasif@hotmail.com, afzaalasn@gmail.com, shahbaz_nazir1@yahoo.com, khwajamutahir311@gmail.com

Abstract:

Incidents among road vehicles happen raised measures of wounds, passing rates, and vital cash related losses. Vehicle to everything updates road prosperity, traffic stream, Traffic adequacy, roadway security, and communication unflinching quality or decreases traffic blocking which impacts transportation. Vehicular Ad-hoc networks is a huge thought from the investigation organize and the vehicle business to improve the organizations of cooperate intelligent transportation system. The potential results of vehicle-to-vehicle, vehicle-to-structure, vehicle to cloud, vehicle to house, vehicle to network, vehicle to pedestrian correspondence showing, and PC entertainment will be shown. A quick generation of vehicular Ad-hoc masterminds is continuously required. In any case, this is nothing yet hard to achieve in light of the way that road traffic and framework correspondence test frameworks are amazing and normally creamer structures are required. One such a mutt approach, Vehicles in Network Simulation (Veins), melds the by and large used Simulation of Urban Mobility and the renowned discrete event multiplication state of Objective Modular Network Testbed in C++ (OMNET++).

Keywords:

Transportation system; V2X; Vehicular Ad-hoc networks; Communication protocol

1. Introduction

Every year millions of people died due to a road accident or millions were annually injured in traffic accidents. With the passage of time, the number of vehicles was rapidly increasing on community roads. Traffic growing increase fuel consumption, Traffic jam, pollution, and Traffic consumption. With the high rate of traffic, many people lost their lives in a road accident. Vehicle-to-Everything (V2X) technology allows cars to connect with their environments or creates the driving harmless or much more efficient for each person. Either the invisible or visible V2X informs the driver of highway threats that can be helpful to decrease traffic injuries or death rates. It improves road safety, traffic efficiency, and comfortability of vehicles. V2X helps to enhance traffic flow, reduce traffic blocking, and lessen environmental which impacts transportation [1][2][3].

To decrease the environmental pollution through the technological progress of research and area growth of Autonomous and cooperative driving. Autonomous driving has the main objective that vehicles have their sensors, which observe the environment as radars, cameras, and Global Positioning System (GPS). The constraint of proximity sensors, which only detects the line-of-sight object [4]. Cooperative driving has significant technology, which increases their traffic efficiency and safety.

To improve communication reliability, Traffic efficiency, Roadway safety through VANET technology with the approach of hybrid and Vehicle in Network Simulation (Veins) which combines the Simulation of Urban Mobility (SUMO) and distinguished isolated event simulation environment OMNET++. Possibilities of vehicle-to-Everything (V2X) communication modeling and computer simulation will be used through VANET technology [5].

Nowadays autonomous driving is an emerging and one of the fastest-growing technologies of 5th generation mobile networks. Vehicle-to-Everything or V2X communication protocol helps with self-driving cars. It supports the V2P, V2N, V2V, V2H, and V2C communication. This allows the self-driving cars to communicate with each other. This will allow self-driving cars to interact like human beings. V2X is expected to provide different services like automated driving, traffic efficiency, and road safety service. Communication of

V2X is a challenging task that requires more attention now a day. We have to design a communication protocol for the automated vehicular system that allows the vehicle control system to perform more efficient decisions based on V2Xcommunication and behavior.

The rest of the paper is organized as follows: Section II gives an overview of the previous work. Basic concepts related to our research, research methodology and various vehicle networks are introduced in Section III. The results and discussions are presented in Section IV. The final conclusions and future work have been described in Section V.

2. Related Work

In 2015 Atallah, R. F. and Khabbaz proposed in this direction, ITS vehicular systems necessities, and effectively noticed IEEE 802.11p innovation [6] that has 27 Mbps most extreme throughput with V2X applications. As an option, the Long-Term Evolution (LTE) innovation has been utilized to help vehicle applications [7], anyway, the exhibition is influenced by obstruction as appeared by [8]. In 2017 Miss. Komal V. Dhole et al. proposed Vehicular Ad-hoc Networks noteworthy thought investigation organize vehicle business recover organizations of the intelligent transportation system. Quick reenactment of Vehicular uncommonly named frameworks (VANETs) is logically required. Regardless, this is nothing yet hard to achieve in light of the way that road traffic and framework correspondence test frameworks are incredible, and as often as possible creamer structures are compulsory. The unique approach of Veins in Vehicle Network Simulation merges extensively recycled SUMO and the prominent separate occasion reenactment condition OMNET++ [9]. To better learning, for better prediction techniques results were analyzed.

3. Materials and Methods

In this section proposed methodology is discussed as well as it is discussed that which network tool and which method is adopted. Furthermore, Network simulators and framework comparison is done. Cellular-based C-V2X technology is superior to WLAN based in terms of communication range, performance, and reliability.

Knowledge of this vehicle depends on a huge scope on the level of automation. If it is a fully autonomous vehicle, this system must track lanes, obstacles, and additional vehicles, traffic lights, road conditions, pedestrians, and speed limits. The system can be used to estimate the idea of this thesis has longitudinal protections, side interactions with the car, it needs to be done physically. This constraint decreases the number of sensors essential to drive robotically. The perception of the test vehicle provides the data collection of embedded radar and data from other vehicles received through the communication of V2V.

3.1. SUMO

The Simulator for Urban Mobility can precisely display the vehicular traffic, signals. SUMO can be utilized freely without Omnet++ or some other test system. For the most part, the traffic examples or versatility follows made by SUMO can be transported into a few of the prominent system test systems including Omnet++ to make practical vehicle and traffic elements. At long last, Veins are only a lot of expansions solely composed for Omnet++ [10]. As such, Veins is one of the model libraries composed of Omnet++, which will give a lot of conventions to recreate VANET under Omnet++. Veins will work alongside SUMO and can utilize its traffic models (portability situations and examples) under Omnet in an all-around coordinated mold [11]. By joining the all the over three, we can complete an extremely sensible vehicles to vehicles (V2V), vehicles to a framework (V2I), vehicles to people on foot (V2P), vehicles to home (V2H), and Vehicle-to-Everything (V2X) organize reproductions on any reasonable guide with practical system convention stacks.

3.2. Network Simulator

NS-2 (Network Simulator 2) is a reliably utilized discrete occasion that arranges the test system. It utilizes the C++ duplication part and Object-sorted out Tool Command Language (OTCL) for reenactment outlining. It is open-source; thusly, new modules are certainly not difficult to figure it out. Remote help wires focus point versatility, spread appearing for radio, and 802.11p show. NS-2 in like way bolster the occasion scheduler, which keeps up the occasion log and executes the augmentation in like manner.

3.3. VANET Simulator

VEINS (Vehicles in Network Simulation) is an open-source VANET structure that utilizations SUMO as the adaptability generator and OMNeT++ as the system test structure. VEINS is bidirectionally coupled among system and traffic test structures empowering it to demonstrate the impact of street traffic on system traffic furthermore the distinctive way. For instance, vehicles need to change their course or back off (change in adaptability arrangement) on get-together of a notice message made by the system test structure. Message trade between adaptability generator and

system test structure happens to utilize TCP. Confirmed maps can be utilized for street arrangement plans. Besides, a characteristic application has in addition been joined that screens the carbon dioxide gas discharged by the vehicles.

3.4. Testing

MANET++ applications utilizing VENIS data could be first recreated in the CLOsed-loop Parallel Simulator (CLOPS) and afterward approved utilizing genuine roadway sensor information through HILS. To catch the development of the non-CVs, a few sorts of locators can be utilized, for example, the magnetometer, inductive circle identification (ILD), video recognition, and so forth. Circle identification is likewise fit for tallying traffic. In any case, it isn't 100% solid for real traffic includes in light of the fact that the circles in the adjoining through paths are regularly integrated for one yield for the development. To take care of this issue, the most recent video location innovation equipped for checking real traffic can go about as a supplement for the circle indicator. Figures 1 (a) and 2 (b) demonstrates how the two programmings distinguish vehicles at the crossing point through programming. Since the objective is to reenact the two CVs and non-CVs, it is important to nourish the vehicles' data to the traffic and correspondence test systems. The RSU can consequently distinguish the CVs from the BSM bundles, however, the circle recognition and video discovery methods are important for identifying the non-CVs. When the RSU gets the information from every one of the sources (for example BSM parcels, inductive circle, video, and magnetometer), a sifting calculation isolates the non-CVs from the CVs utilizing the BSM bundles. There is a re-distinguishing proof issue regarding the utilization of circle indicator, video discovery, and magnetometer. To kill the re-recognizable proof issue, we will unite the roadway sensor information from three sources alongside CV information to precisely distinguish the two CVs and non-CVs. In any case, the discovery of the non-CV is not adequate for the equipment in circle reproduction. The versatility hint of a non-CV between two crossing points is required. A vehicle following a model between one/two CVs and a non-CV can be utilized to extrapolate the missing hint of a non-CV vehicle. For instance, the missing portability hint of a non-CV vehicle can be extrapolated utilizing two CVs' versatility follows where one CV goes before the non-CV and one CV that pursues the non-CV. All the more for the most part, we can use the current stochastic or probabilistic traffic stream and portability follow recreation strategies [12][13][14] to reproduce the versatility hints of the non-CV vehicles considering the CV vehicles as the test vehicles (subtleties talked about in the second test of HILS). Different sensors in a crossing point can help to refine the recreation. Fig.2 demonstrates the progression of sensor information for equipment on the up and up reenactment.

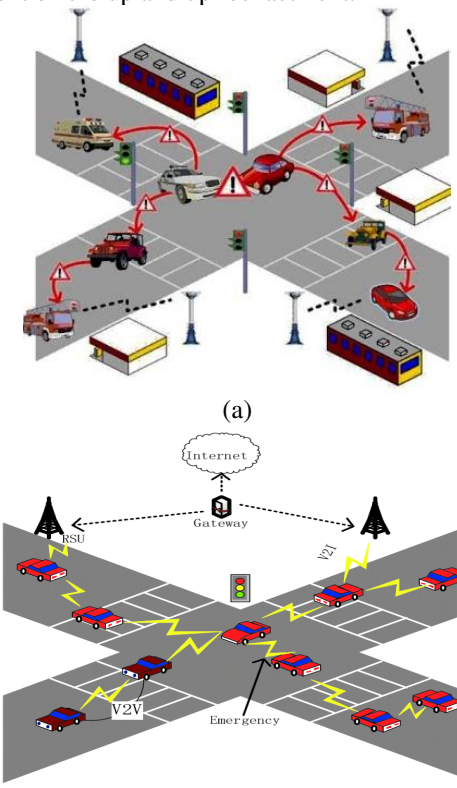


Fig.1 (a)(b) Sensor data for hardware-in-the-loop simulation

A portion of the investigations related to partaking equipment tuned in a generation are depicted underneath: 1) Isolating CV traces from loop-discovery and video detection information The hardware-on top of it simulation (HILS) technique can capture roadway sensor information from four different sources DSRC broadcast messages, inductive circles, video detectors, and wireless magnetometers. Shockingly, the roadway sensors at intersections cannot differentiate between a CV and non-CV. In this way, a solid filtering mechanical assembly is expected to recognize the CVs among all the traffic by clearing out the CV information from other two sensors' information dependent on the GPS position and circle detection timings.

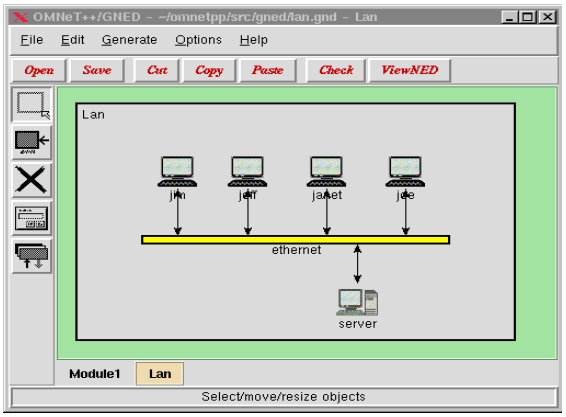


Fig.2 Sensor data for hardware-in-the-loop simulation

4. Result and Discussion

The reproduction with referenced situations has been done and the voyaging times for each of the 20 vehicles have been gotten. Fig.5 demonstrates the information, which was acquired in the past segments utilizing SUMO. Furthermore, the Probability of Beacon Delivery (PBD) for 20 vehicles is determined to break down the precision of MANET reproduction. PBD is determined by thinking about all the lost reference points and got guides amid the adventure for every vehicle from its starting point to the goal. Additionally, for every one of the referenced 20 vehicles, the contrast between voyaging time in SUMO and OMNET++ test system are considered. Fig.1 (a) and Fig. (b) shows the way that the distinction between traffic reenactment result (perfect) and VANET reproduction result (sensible) is very little. Practical outcomes are gathered from the recreation with system test system (OMNET++) by utilizing the beaconing and IEEE 802.11p standard. The created program is utilized SUMO to get the perfect structure which thinks about the definite CVs (voyaging time) and the precise position of the autos and RSUs for changing the courses. This Accurate and worthy outcome has a few reasons, one of them is identified with various communication.

CLOsed-loop Parallel Simulator (CLOPS) and the contrast between voyaging times got from SUMO and OMNET++ test system utilizing DRP Messages in the beaconing situation, which intends to convey the data to different vehicles and RSUs soon. This reality demonstrates that V2X and V2V correspondence utilizing IEEE 802.11p and utilizing CLOPS is fit to diminish the voyaging time of the vehicles. Also, Fig. 5 represents that with expanding the traffic thickness the PBD is diminished and the autos voyaging time is expanded.

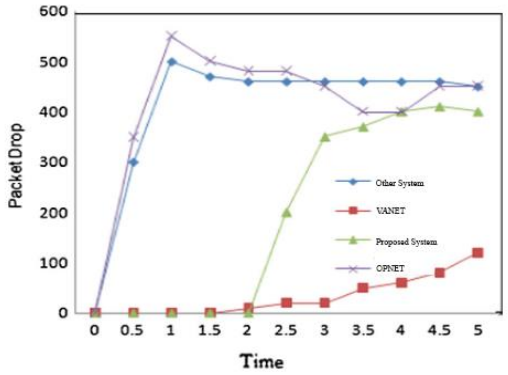


Fig.3 Packet drop vs. time

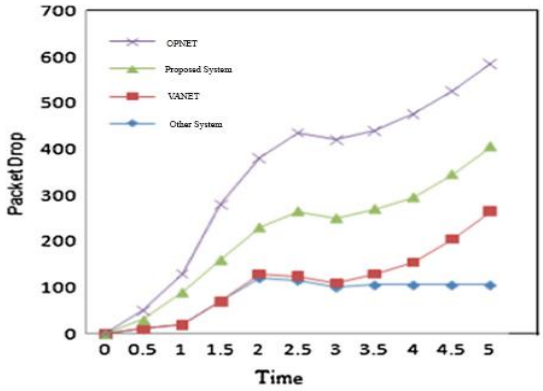


Fig.4 Throughput in kb/s vs. time in sec

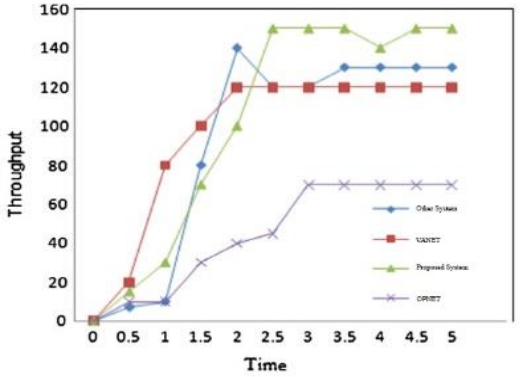


Fig.5 Packet icollision irate vs. itime

5. Conclusion and future work

In this paper, we initially raise factors that different impersonating VANET from appearing customary MANET. We illuminate the choice of depicting traffic at moment measurement and we present assorted features that could be consolidated into such a vehicular adaptability model. We orchestrate particular proliferation instruments subject to

how they are executed. For each class, we talk about regular traits and the particularities of each system.

VANET is never again a remote possibility; given that mind-boggling hypotheses are currently in the pipeline from a couple of divisions including government workplaces, vehicle undertakings, course security, and open transport specialists. Particular fitting authoritative workplaces are working personally with vehicle makers/adventures.

References

[1] T. Rosenstatter and C. Englund, "Modelling the Level of Trust in a Cooperative Automated Vehicle Control System," IEEE Trans. Intell. Transp. Syst., 2018.

[2] T. Nguyen, A. Islam, T. Hossan, and Y. M. Jang, "Current status and performance analysis of optical camera communication technologies for 5G networks," IEEE Access, 2017.

[3] M. A. Saleem et al., "Expansion of Cluster Head Stability Using Fuzzy in Cognitive Radio CR-VANET," IEEE Access, vol. 7, pp. 173185–173195, 2019.

[4] M. A. Saleem, Z. Shijie, and A. Sharif, "Data Transmission Using IoT in Vehicular Ad-Hoc Networks in Smart City Congestion," Mob. Networks Appl., vol. 24, no. 1, 2019.

[5] B. M. Masini, A. Bazzi, and A. Zanella, "A survey on the roadmap to mandate on board connectivity and enable V2V-based vehicular sensor networks," Sensors (Switzerland), 2018.

[6] J. Lianghai, A. Weinand, B. Han, and H. D. Schotten, "Applying Multiradio Access Technologies for Reliability Enhancement in Vehicle-to-Everything Communication," IEEE Access, 2018.

[7] K. Ganesan, P. B. Mallick, J. Lohr, D. Karampatsis, and A. Kunz, "5G V2X Architecture and Radio Aspects," in 2019 IEEE Conference on Standards for Communications and Networking, CSCN 2019, 2019.

[8] S. Y. Gelbal, S. Arslan, H. Wang, B. Aksun-Guvenc, and L. Guvenc, "Elastic band based pedestrian collision avoidance using V2X communication," in IEEE Intelligent Vehicles Symposium, Proceedings, 2017.

[9] V. Lakshminarayanan, V. G. S. Chemudupati, S. K. Pramanick, and K. Rajashekara, "Real-time optimal energy management controller for electric vehicle integration in workplace microgrid," IEEE Trans. Transp. Electrif., 2019.

[10] A. Sharif, J. Li, M. Khalil, R. Kumar, M. I. Sharif, and A. Sharif, "Internet of things - Smart traffic management system for smart cities using big data analytics," in 2016 13th International Computer Conference on Wavelet Active Media Technology and Information Processing, ICCWAMTIP 2017, 2017.

[11] S. Chen et al., "Vehicle-to-Everything (v2x) Services Supported by LTE-Based Systems and 5G," IEEE Commun. Stand. Mag., 2017.

[12] M. Höyhtyä, O. Apilo, and M. Lasanen, "Review of latest advances in 3GPP standardization: D2D communication in 5G systems and its energy consumption models," Future Internet. 2018.

[13] J. Montalban et al., "Multimedia Multicast Services in 5G Networks: Subgrouping and Non-Orthogonal Multiple Access Techniques," IEEE Commun. Mag., 2018.

[14] A. Ur Rehman Khan, S. M. Bilal, and M. Othman, "A performance comparison of open source network simulators for wireless networks," in Proceedings - 2012 IEEE International Conference on Control System, Computing and Engineering, ICCSCE 2012, 2012.

PATH PLANNING BASED ON CLOTHOID FOR AUTONOMOUS VALET PARKING

SUI LIYANG[1,2,3], YU HOUYU[1,2,3,*], CHEN XUEZHI[1,2,3], JIA CHANGHAO[1,2,3], HUANG MIAOHUA[1,2,3]

[1] Hubei Key Laboratory of Advanced Technology for Automotive Components, Wuhan University of Technology, Hubei 430070, China
[2] Hubei Collaborative Innovation Center for Automotive Components Technology, Wuhan University of Technology, Hubei 430070, China
[3] Hubei Research Center for New Energy & Intelligent Connected Vehicle, Wuhan University of Technology, Hubei 430070, China
E-MAIL: leon_sui@whut.edu.cn, yuhouyu@sina.com

Abstract:

The problem of path planning of the autonomous valet parking can be explained as the planning of a path from the entrance of the parking lot to the parking space. Firstly, by collecting the location information of key nodes in the parking lot, the topological map of the parking lot is defined, which is composed of parking space information and road topological network. Secondly, the reasonable parking space searching path and parking path are planned, and their curvature discontinuity is smoothed. The parking path adopts the C-shaped method, the path of searching for parking spaces adopts the line-arc-line splicing method, and use the clothoid curve to smooth the path. Finally, Stanley path tracking algorithm is used to follow the planned path based on MATLAB to verify the effectiveness of the path planning algorithm. The simulation results show that the proposed algorithm can realize the seamless splicing between the searching path and the parking path, and the planned path can be tracked better.

Keywords:

Autonomous valet parking; Path planning; Clothoid; Path tracking

1. Introduction

Autonomous valet parking system, as a higher level of autonomous driving, is the most promising technology for commercialization in the L4 level, and has also become a research hotspot in academia and industry. If it can be successfully implemented, it will greatly improve the travel efficiency, and can achieve the effect of energy saving and emission reduction.

The intelligent parking can send the parking map and occupied parking space information to autonomous vehicles through the V2I technology, which can reduce the complexity of perception algorithms for autonomous vehicles. Therefore, many researches in the past decade have involved the construction of appropriate digital map [1-3] and parking occupancy rate detection system [4-5] based on the infrastructure. In the aspect of path planning, Klaudt et al. [6] utilized Hybrid A* algorithm to plan the whole searching path and parking path. Min et al. [7] used A* algorithm to search the parking space under the light of predicting the initial parking point, then planned the parking path with an arc, and parked the vehicle by adjusting the steering wheel angle for many times.

Based on the existing parking planning algorithm, this paper proposes a strategy in the coordination of searching path and parking path, so as to make the planned path conform to the driver's habit, with smooth curvature and easy tracking. Firstly, this paper designs a topological map of the parking lot according to relevant parameters, including the key nodes and parking space information in the whole parking lot. Secondly, based on the driver's habit, the parking process is divided into three actions: going straight, turning and reversing. Each action can consist of a straight line and an arc. Thirdly, in order to smooth the path, the clothoid used by the road design engineer is used as the transition curve between the straight line and the arc, so that this planned path with continuous curvature is easy to track.

2. Design of topological map of parking lot

The parking lot topology map established in this paper is shown in Figure.1. A cartesian coordinate system is established by taking O at the lower left corner of the parking lot as the origin of coordinates. Topology map is composed of parking information and road topology network. The parking space information can be expressed as matrix Q, and the road topology network can be expressed as P_m, as shown

in equation 1 and 2.

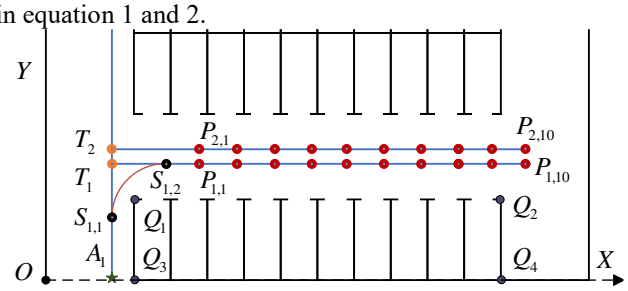


Fig.1 Parking lot topology map

$$Q=\begin{bmatrix} Q_{lr,1} & Q_{rr,1} & Q_{rf,1} & Q_{lr,1} \\ \vdots & \vdots & \vdots & \vdots \\ Q_{lr,N_Q} & Q_{lr,N_Q} & Q_{lr,N_Q} & Q_{lr,N_Q} \end{bmatrix}_{N_Q\times 4} \tag{1}$$

$$P_{\mathrm{m}}=\begin{bmatrix} (x_{A_1},y_{A_1}) \\ (x_{T_1},y_{T_1}) \\ \vdots \\ (x_{T_{N_T}},y_{T_{N_T}}) \\ (x_{P_{1,1}},y_{P_{1,1}}) \\ \vdots \\ (x_{P_{N_T,N_P}},y_{P_{N_T,N_P}}) \end{bmatrix}_{(N_T+N_T\times N_P+1)\times 1} \tag{2}$$

Q is composed of four vertices of each parking space. Q_{lr}, Q_{rr}, Q_{rf} and Q_{lf} respectively represent four vertices of each parking space, including left rear, right rear, right front and left front. The road topology network includes: starting node, steering node, and parking starting node. The starting node is A_1, the steering nodes are T_1~T_{NT}, parking starting node is $P_{1,1}$~$P_{NT,\,NP}$. N_T is the total number of steering nodes and N_P is the number of starting parking points corresponding to each steering node, which can also be regarded as the number of parking spaces per row. In figure 1, A_1 represents the starting node, when the starting node of parking is $P_{1,\,1}$-$P_{1,10}$, the corresponding steering node is T_1. When the starting node of parking is $P_{2,1}$-$P_{2,10}$, the corresponding steering node is T_2. The road topology network satisfies the following rules: $T_1P_{1,10}$ parallels to Q_1Q_2, and Q_1Q_3 parallels to T_1A_1.

3. Path planning algorithm

3.1. Parking path planning

Firstly, the local map of parking is modelled. As shown in the figure 2, coordinate system XO_1Y is established by taking the origin of coordinates, O_1, at the lower left corner of the parking space.

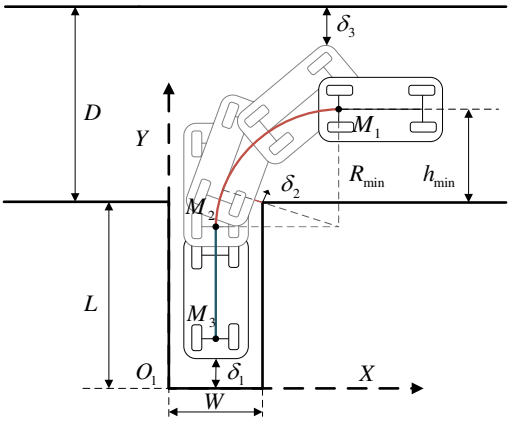


Fig.2 Vertical parking process

In the Figure.2, D is the width of the road, L is the length of the parking space, and W is the width of the parking space, which can be obtained by sending the topology map through V2I technology. δ_1 , δ_2 , δ_3 are the safety distance requirements, which are set artificially but must be greater than or equal to 0. Combined with the vehicle parameters and the above six parameters, three key points M_1, M_2 and M_3 of C-shaped parking path can be calculated. M_1 is the starting point of parking and reversing from this point. M_2 is the point where the vehicle body is parallel to the parking space when reversing. M_3 is the end of the parking process. Referring to [8], the specific coordinates of M_1, M_2 and M_3 can be calculated as equation 3.

$$\begin{aligned} M_1&:\left(\frac{W}{2}+R_{\min},L+R_{\min}-\sqrt{\left(R_{\min}-\frac{W_c}{2}-\delta_2\right)^2-\left(R_{\min}-\frac{W}{2}\right)^2}\right) \\ M_2&:\left(\frac{W}{2},L-\sqrt{\left(R_{\min}-\frac{W_c}{2}-\delta_2\right)^2-\left(R_{\min}-\frac{W}{2}\right)^2}\right) \\ M_3&:\left(\frac{W}{2},\delta_1+\mathrm{L_r}\right) \end{aligned} \tag{3}$$

L_r is the rear overhang distance, W_c is the width of the vehicle, and R_{min} is the minimum turning radius of the center of the rear axle. This method is relatively simple, but in practice, if you want to track this path, you need to turn the steering wheel to the right full at the point M_1 and then start reversing, stop at the point M_2 and then reverse. It is not consistent with the driver's parking habits and will increase the parking time, so it needs to be optimized. To solve the problem of discontinuous path curvature, a method based on clothoid splicing arc is proposed in this paper. Clothoid [9] is the curve whose curvature increases linearly with the length of the curve. The definition of curve change rate is as follows:

$$c=\frac{\rho}{s}=\frac{1}{Rs} \tag{4}$$

In the equation 4, s is the length of the clothoid, ρ is the curvature at the end point of the clothoid, R is the radius of curvature at the end point of the clothoid, and c is the curvature change rate. If the longitudinal speed of the vehicle and the change rate of the front wheel angle is constant, the track of the rear axle of the vehicle can be regarded as a clothoid curve, then the requirement of continuous change of curvature can be satisfied. As shown in the Figure.3, when stitching a clothoid and an arc, it is necessary to determine the coordinates at the point where the clothoid and the arc are spliced together, as well as the lateral offset n_1 and longitudinal offset n_2 of the starting coordinates of the clothoid and the initial coordinates of the arc. The local coordinate system XO_3Y is established with the origin point O_3, which is the start of the clothoid, and the curvature at point O_3 is 0. Point G_1 is the end point of the clothoid O_3G_1, and also a point on the arc with the radius of R_{min}, with the curvature of $1/R_{min}$.

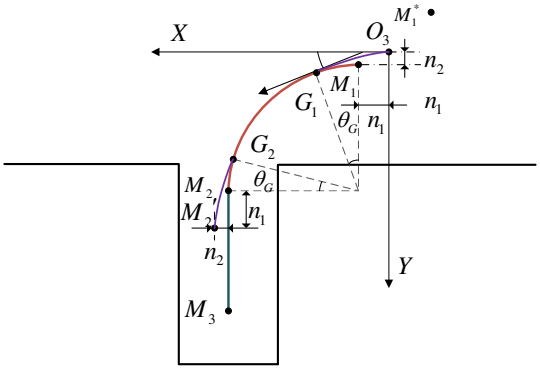


Fig.3 Parking process based on clothoid

The position of point G_1 on the curve G_1G_2 can be expressed as equation 5.

$$\begin{cases} A=\sqrt{1/c} \\ x_G=A\sqrt{\pi}\int_0^{\frac{1}{\pi A}}\cos(\pi/2)u^2du \\ y_G=A\sqrt{\pi}\int_0^{\frac{1}{\pi A}}\sin(\pi/2)u^2du \\ \theta_G=\dfrac{1}{2R^2c^2} \end{cases} \tag{5}$$

According to the geometric relationship, n_1 and n_2 can be calculated from the equation 6 and 7.

$$n_1=x_G-R_{\min}\theta_G \tag{6}$$

$$n_2=y_G-R_{\min}(1-\cos\theta_G) \tag{7}$$

The actual parking path needs to be corrected by adding two clothoids at M_1 and M_2. The principle of the correction is that the whole curve shifts to the top right, so that the coordinates of M_2' are equal to those of M_2. The optimized starting point M_1* is shown in Figure.3, and it can be expressed as equation 8.

$$M_1^*=(x_{M1}+n_1+n_2,\ y_{M1}+n_1+n_2) \tag{8}$$

3.2. Path planning of searching parking spaces

The searching process of parking spaces can be divided into two actions of straight going and turning in behavioral decision making, so determination of the coordinate of point T_i when turning at the intersection is the key in this section. According to the principle defined in the topology map, the y-coordinate of point T_i is equal to the corresponding y-coordinate of the starting point of parking. When the maximum curvature during turning is $1/R_{min}$, the turning process can be regarded as the C-shaped parking process, and the collision point is the Q_1 in the Figure.4. Considering that the width of one-way road is generally greater than the width of the parking space, so the vehicle in the main road when keeping straight in the lane center line will not collide at the corner, the x coordinate of point T_i is equal to $3D/4$. At this point, the coordinates of point T_i can be determined. After obtaining the equation 2, the adjacency matrix A_m of the P_m can be determined as equation 9.

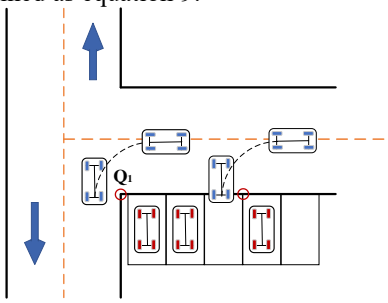


Fig.4 Turning process at intersection

$$A_{\mathrm{m}}=\begin{bmatrix} a_{1,1} & \cdots & a_{1,N_m} \\ \cdots & a_{i,j} & \cdots \\ a_{N_m,1} & \cdots & a_{N_m,N_m} \end{bmatrix}_{N_m\times N_m} \tag{9}$$

a_{ij} represents the distance between the ith node and the jth node. If the two nodes are not adjacent, then $a_{ij}=\infty$. Given the initial node and the parking starting node, according to A_m, Dijkstra algorithm can be used to obtain the shortest path from the initial point to the target parking point. However, the method is not easy to track because of the right-turn path at the corner, so it needs to be optimized. Using the optimization method in parking process for reference, this paper adopts the combined method of clothoid-arc-clothoid to complete the transition of turning. The radius of the arc is

R_{min}. Assuming that the vehicle speed and the steering wheel angle don't change during the parking process, the path curve during turning can be obtained by translating the parking path. Point T_1 in the Figure.1 is taken as an example. The coordinates of the optimized endpoints $S_{1,1}$ can be expressed as equation 10.

$$S_{1,1}=(x_{T_1},\ L-\sqrt{\left(R_{\min}-\frac{W_c}{2}-\delta_2\right)^2-\left(R_{\min}-\frac{W}{2}\right)^2}) \quad (10)$$

The smoothed turning path can be expressed by $S_{1,1}S_{1,2}$ in figure 1.

4. Path tracking

In the parking process, the vehicle speed is very low, so it is unnecessary to consider the dynamic constraints of the vehicle. The path tracking algorithm is simple and real-time, and can keep good tracking accuracy at low speed. Therefore, the path tracking algorithm based on Stanley model [10] shown in Figure.5 is selected in this paper. The Stanley lateral controller can be expressed as equation 11.

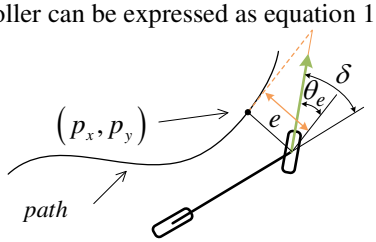


Fig.5 Stanley model

$$\delta(t)=\theta_e(t)+\arctan\frac{k\times e(t)}{v(t)} \quad (11)$$

Where e is the distance from the centre of the front axis to the nearest path point (p_x, p_y). θ_e represents the angle between the vehicle heading and the tangential direction of the nearest path point. δ is the front wheel angle, k is the gain coefficient. Better tracking accuracy can be achieved by adjusting the value of k.

5. Simulation and results

Table 1 Vehicle model parameters

Vehicle length	4.540m	Rear overhang	0.930m
Vehicle width	1.831m	Minimum turning radius	4.292m
Wheelbase	2.670m	Front overhang	0.940m

In this paper, an occupancy grid map is established by MATLAB. The size of the map is 39m×34m，the width of the road is 6m, the length and width of each parking space are 5.4m and 2.4m respectively. The parameters of the simulated vehicle are shown in the Table 1.

The target parking space is selected as the sixth parking space in the first row, and simulation results can be obtained as shown in the figure 6 to 8.

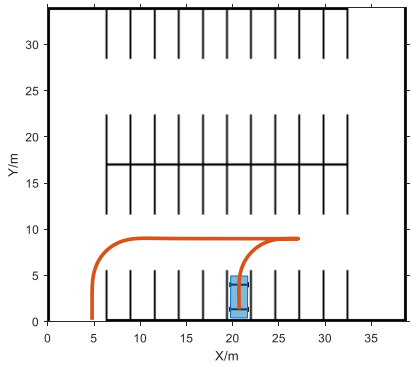


Fig.6 Path planning results

Figure.6 shows the track of the vehicle from the starting point of parking lot to the target parking space. Figure.7 shows the deviation between the reference track and the actual track during the reversing process, and Figure.8 shows the equivalent front wheel angle during the reversing process. It can be seen that the planned path can be easily tracked, the change of equivalent front wheel angle is relatively smooth, and the tracking error is within 5cm.

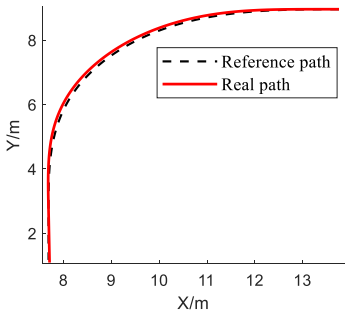


Fig.7 Deviation of path tracking

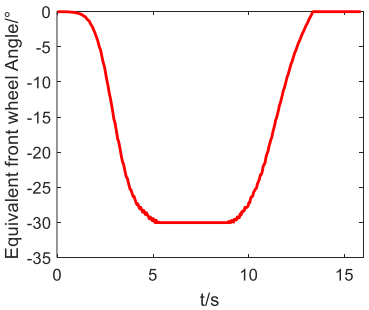


Fig.8 Equivalent front wheel angle

6. Conclusion

This paper studies the path planning of autonomous valet parking system. First, a topological map of the parking lot is defined. Secondly, the clothoid curve is used to optimize the parking path and searching path for parking space. Finally, the path tracking and its simulation are carried out based on Stanley lateral controller. The simulation results show that the equivalent front wheel angle changes steadily and the tracking error is small, and the vehicle can smoothly and accurately complete the process of searching parking space and reversing into parking space.

Acknowledgements

This work is funded by the Fundamental Research Funds for the Central Universities, under Grant No. 205207002.

References

[1] Schreiber M, Knöppel C,and Franke U, "Laneloc: Lane marking based localization using highly accurate maps", 2013 IEEE Intelligent Vehicles Symposium, Gold Coast, pp.449-454, June 2013.

[2] Tao Z, Bonnifait P, Fremont V, et al, "Lane marking aided vehicle localization", 16th International IEEE Conference on Intelligent Transportation Systems, Hague, pp.1509-1515, October 2013.

[3] Fabian T, "An algorithm for parking lot occupation detection", 2008 7th Computer Information Systems and Industrial Management Applications, Ostrava, pp.165-170, June 2008.

[4] Gruyer D, Belaroussi R, et al. "Map-aided localization with lateral perception", 2014 IEEE Intelligent Vehicles Symposium, Dearborn, pp.674-680, June 2014.

[5] Bulan O, Loce R P, et al, "Video-based real-time on-street parking occupancy detection system", Journal of Electronic Imaging, 22(4), pp. 0411091-04110915, August 2013.

[6] Klaudt S, Zlocki A, Eckstein L, "A-Priori map information and path planning for automated valet-parking", 2017 IEEE Intelligent Vehicles Symposium, Redondo Beach, pp.1770-1775, June 2017.

[7] Min K W, Choi J D, "Design and implementation of an intelligent vehicle system for autonomous valet parking service", 2015 10th Asian Control Conference, Kota Kinabalu, pp.1-6, May 2015.

[8] Si Sun, "Research on Steering Control Strategy of Automatic Vertical Parking System", Tsinghua University, 2015.

[9] Muller B, Deutscher J, et al, "Continuous curvature trajectory design and feedforward control for parking a car", IEEE Transactions on Control Systems Technology, 15(3), pp.541-553, April 2007.

[10] Thrun S , Montemerlo M , et al, "Stanley: the robot that won the DARPA grand challenge", Journal of Field Robotics, 23(9), pp.661-692, September 2006.

AN AUTONOMOUS VEHICLE MOTION PLANNING METHOD BASED ON DYNAMIC PROGRAMMING

JIA CHANGHAO[1,2,3], HUANG MIAOHUA[1,2,3*], SUI LIYANG[1,2,3]

[1] Hubei Key Laboratory of Advanced Technology for Automotive Components, Wuhan University of Technology, Wuhan 430070, China

[2] Hubei Collaborative Innovation Center for Automotive Components Technology, Wuhan University of Technology, Wuhan 430070, China

[3] Hubei Research Center for New Energy & Intelligent Connected Vehicle, Wuhan University of Technology, Wuhan 430070, China

E-MAIL: changhao.jia@whut.edu.cn, mh_huang@163.com, leon_sui@whut.edu.cn

Abstract:

In this article, we propose a new approach to solve local motion planning problem in autonomous vehicle field. Instead of generating several primitives and choosing the optimal trajectory from that, we get the future T time step horizon's vehicle state, and fit that into clothoid local trajectory by solving a dynamic programming problem. The trajectory generated is smooth enough and meet both ego vehicle's dynamics and traffic regulation's constraints. Iterate this process, the ego autonomous vehicle can obtain its future trajectory continuously. This method has a good performance in the simulation using Matlab and Prescan. This method has fast computing speed to apply on autonomous vehicle driving in real road online compared to other methods.

Keywords:

Autonomous vehicle; Motion planning; Clothoid curve; Dynamic programming

1. Introduction

Traffic accidents have been a major threaten on people's life and health, and wrong driving behavior is the most important reason causing it. Autonomous vehicles can avoid most traffic accidents without human inappropriate driving behavior. The autonomous vehicle technique mainly includes perception, localization, prediction, planning and control. The planning module is one of the most important and challenging module. The motion planning module receive info from perception, localization and prediction modules' output as it's input. The output of planning modules is the trajectory which will be transfer to control module as it's input, and make the autonomous vehicle driving autonomously. The trajectory generated by planning modules have information of two aspects. One is the geometric path, and the other is the speed profile corresponding to the path.

In motion planning modules, the process generally consists of two steps [1]. First, using start position, end position and map information as input to generate the global route that has short driving distance and little traffic congestion. We call this step route planning in this paper. Second, because that the global route is a sequence of points on geometric, it may not constrain to the vehicle dynamics model and the global route has no speed information. The local motion planning modules which we call trajectory planning in this article use the global route, ego vehicle's current position which provided by the localization modules, static obstacles' position which provided by the perception modules and the dynamic obstacles' trajectory possibility distribution provided by the prediction modules as it's input, and output the trajectory to the control modules over a T time step horizon. The scheme of the motion planning modules can be described as Figure 1.

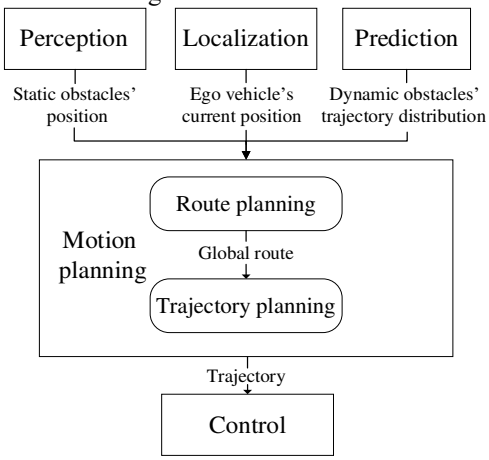


Fig.1 A scheme of autonomous vehicle motion planning module

To solve the trajectory planning problem, we propose a new approach based on dynamic programming. The organization of this article is as follows: First, in section 2, we give the accurate problem formulation, in which we describe the problem assumptions, introduce the G^1 clothoid fitting method and derive the ego vehicle's kinematic model and it's state-space representation. Then, in section 3, we illustrate the trajectory generation approach, in which we use the deviation from the reference line, estimated distance to obstacles, and constraints of traffic regulations to define the cost function, and get the optimization statement. Then, in section 4, we use Matlab and Prescan to conduct a simulation experiment, in which we give the parameters used in simulation, and show the simulation results. Finally, Section 5 gives the conclusion of this article.

2. Problem formulation

2.1. Assumptions

This article mainly focus on the local motion planning modules. We assume that the autonomous vehicle trajectory planning module has the following information: The perception modules provide the static obstacles' position near the ego autonomous vehicle. The localization modules provide the map information which includes road boundaries, lane width, lane line position etc. and ego vehicle's current location coordinates. The prediction modules provide the dynamic obstacles' trajectory possibility distribution over a T time step horizon. The route planning modules provide the global route path from starting point to the goal point.

2.2. Clothoid fitting reference line

The route planning modules' output is a sequence of points' coordinates geometrically that don't have speed profile information. The output of route planning modules can be expressed as formula (1).

$$G = \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ y_1 & y_2 & \cdots & y_n \end{bmatrix}. \tag{1}$$

Where $G_1(x_1, y_1)$ and $G_n(x_n, y_n)$ are the starting point and end point of the global route respectively. There are several ways fitting these discrete points into a smooth curve such as sigmoid [2], polynomial [3], spline [4] and Bezier curve [5]. We use clothoid curve to fit G into the reference line for trajectory planning in this article. G can be fitted to n-1 separate clothoid curves [6], the i-th reference line can be given by formula (2).

$$\begin{cases} x_{ref}(s) = x_i + \int_0^s \cos(\frac{1}{2}\kappa_i\tau^2 + \psi_i\tau + \beta_i)d\tau, \\ y_{ref}(s) = y_i + \int_0^s \sin(\frac{1}{2}\kappa_i\tau^2 + \psi_i\tau + \beta_i)d\tau. \end{cases} \tag{2}$$

Where s denotes the arc length from $G_i(x_i, y_i)$, $\kappa_i + \psi_i$ denotes the curvature of this segment and β_i denotes the starting points' heading angle. The i-th curve's end points' curvature is as same as the (i+1)-th curve's starting points' curvature. In each segment, the problem can be described as: Given two points $G_i(x_i, y_i)$ and $G_{i+1}(x_{i+1}, y_{i+1})$ and two angles β_i and β_{i+1}, find a clothoid segment of formula (2) that satisfies formula (3).

$$\begin{cases} x(0) = x_i,\ y(0) = y_i, \arctan(\frac{y'(0)}{x'(0)}) = \beta_i. \\ x(L_i) = x_{i+1},\ y(L_i) = y_{i+1}, \arctan(\frac{y'(L_i)}{x'(L_i)}) = \beta_{i+1}. \end{cases} \tag{3}$$

Where L_i denotes the arc length of the i-th reference line. We use the G^1 clothoid fitting method [7] to fit the global reference line in this article.

2.3. Ego vehicle kinematic model

We use the kinematic bicycle model to represent ego vehicle [8]. This model is often used as vehicle kinematic model because of its good performance on expressing vehicle model. This model is shown in Figure 2.

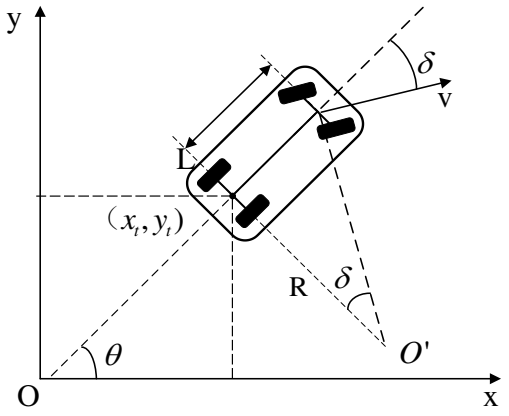


Fig.2 Vehicle kinematic bicycle model

The state-space representation is given by formula (4).

$$\dot{X} = AX + BU$$

$$X = \begin{bmatrix} x \\ y \\ v \\ \theta \\ \delta \end{bmatrix} \quad \dot{X} = \begin{bmatrix} v\cos\theta \\ v\sin\theta \\ a \\ v\dfrac{\tan\delta}{L} \\ u_\delta \end{bmatrix} \quad U = \begin{bmatrix} a \\ u_\delta \end{bmatrix} \tag{4}$$

Where x, y denotes the global coordinates of the ego vehicle. v denotes the ego vehicle's speed. θ denotes the heading angle in the global coordinates. δ denotes the front steering angle in the global coordinates. a denotes the acceleration. u_δ denotes the rate of change of the steering angle. L denotes the ego vehicle's wheelbase. The A and B are both Jacobian matrix that can be calculated by

$$A = \frac{\partial \dot{X}}{\partial X}\Big|_{X=X_0} \qquad B = \frac{\partial \dot{X}}{\partial U}\Big|_{X=X_0} . \tag{5}$$

Where X_0 is the initial state of ego vehicle in formula (5). But this is a continuous time model, to make this method apply on the real scenarios, we must convert it to a discrete system which is given by

$$X(t+1) = F[X(t), U(t)] . \tag{6}$$

From formula (6), we can see that ego vehicle's state X is a function of its former time's state X and control input U.

3. Trajectory generation

To Generate the optimal trajectory, we need to find the ego vehicle state's optimal solution of the cost function. The cost function should contain the following parts: deviation from the reference line, estimated distance to obstacles, and constraints of traffic regulations. We can find the optimal vechicle control over the next T step horizon. Then use formula (6) to get the vehicle state. By fitting the coordinates of X into clothoid curve using method in section 2.2, we can generate the optimal trajectory which has the speed profile.

3.1. Deviation from the reference line

The reference line we fitted is along the center of the road basically. The local trajectory we're planning need to close to the reference line as possible under the condition of no collision and vehicle dynamics [9].

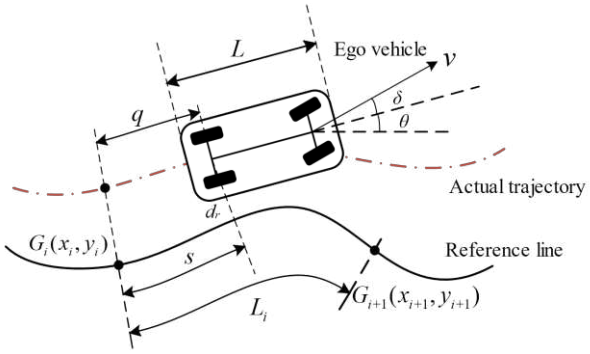


Fig.3 Illustration of deviation from reference line

Figure 3 illustrates the deviation from the reference line. q denotes the actual distance the vehicle has travelled. d_r denotes the deviation to the reference line. The heading angle at points on the reference line, denoted as $\vartheta(s)$, can be calculated by formula (7).

$$\vartheta(s) = \arctan\left(\frac{\dfrac{\delta y_{ref}(s)}{\delta s}}{\dfrac{\delta x_{ref}(s)}{\delta s}}\right) . \tag{7}$$

Where $\frac{\delta x_{ref}(s)}{\delta s}$ and $\frac{\delta y_{ref}(s)}{\delta s}$ denote the derivative of $x_{ref}(s)$ to s and $y_{ref}(s)$ to s respectively. The deviation to the reference line at time t can be approximated with

$$\begin{aligned} \Delta x_t &= x_t - x_{ref}(q) \\ \Delta y_t &= y_t - y_{ref}(q) \\ d_r(t) &= \Delta x_t \sin[\vartheta(s_t)] - \Delta y_t \cos[\vartheta(s_t)] \end{aligned} . \tag{8}$$

3.2. Estimated distance to obstacles

The obstacles that ego vehicle need to avoid colliding includes the static obstacle such as roadblocks and dynamic obstacles such as other vehicles, passengers, etc.

1)Estimated distance to static obstacles: We use the Euclidean distance to express the distance to static obstacles, which can be calculated by

$$d_{so}(t) = \sum_{i=1}^{N_{so}} \sqrt{(x_t - x_i)^2 + (y_t - y_i)^2} . \tag{9}$$

Where (x_i, y_i) is the i-th static obstacle's global coordinate. N_{so} is the number of static obstacles that provided by perception modules.

2)Estimated distance to dynamic obstacles: The prediction modules provide the dynamic obstacle's global coordinates at time t can be expressed at a joint binary possibility distribution. We denote the i-th dynamic obstacles' possibility density function as $p_i(t) = f(x_i(t), y(t))$. Then the distance to dynamic obstacles can be approximated with

$$d_{do}(t) = \sum_{i=1}^{N_{do}} p_i(t)\sqrt{(x_t - x_i(t))^2 + (y_t - y_i(t))^2} \quad (10)$$

In formula (10), (x_i, y_i) is the i-th dynamic obstacle's global coordinate. N_{do} is the number of dynamic obstacles that provided by prediction modules.

3.3. Constraints of traffic regulations

The ego autonomous vehicle must obey the constraints of traffic regulations. The vehicle's trajectory must be in the road line, and the speed of vehicle must meet the road limit. The constrains can be given by formula (11).

$$\begin{aligned} X_{\min} \le X[t+1:t+T] \le X_{\max} \\ U_{\min} \le U[t:t+T-1] \le U_{\max} \end{aligned} \quad (11)$$

3.4. Optimization Statement

For now, the trajectory planning problem can be described as: Given the initial vehicle state X_t and the trajectory planning time step horizon T, find the $U[t:t+T-1]$ that minimize the cost function and satisfy the constrains of regulations. Iterating this process, we can continuously perform local trajectory planning and apply this method online on the real road. This is a dynamic programming problem. The optimization statement can be given by formula (12).

$$\begin{aligned} &\min \sum_{0}^{T} c(X_t, U_t) \\ s.t. \quad &X(t+1) = F[X(t), U(t)] \\ &X_{\min} \le X[t+1:t+T] \le X_{\max} \\ &U_{\min} \le U[t:t+T-1] \le U_{\max} \end{aligned} \quad (12)$$

Where $c(X_t, U_t)$ is the cost function to be optimized that is given by formula (13).

$$c(X_t, U_t) = \omega_1 d_r(t) + \frac{\omega_2}{d_{so}(t)} + \frac{\omega_3}{d_{do}(t)}. \quad (13)$$

Where ω_1, ω_2 and ω_3 are the weight parameters for the deviation from the reference line, estimated distance to static obstacles and dynamic obstacles respectively.

4. Simulation

4.1. Simulation conditions

We use the Prescan to generate the scenario of traffic roads, and Matlab to solve the mathematical optimization problem, generate the trajectory path and fit the result which is a sequence of points into the trajectory. The traffic scenario used to simulation is shown in Figure 4. It's a two-way single lane road and across two intersections.

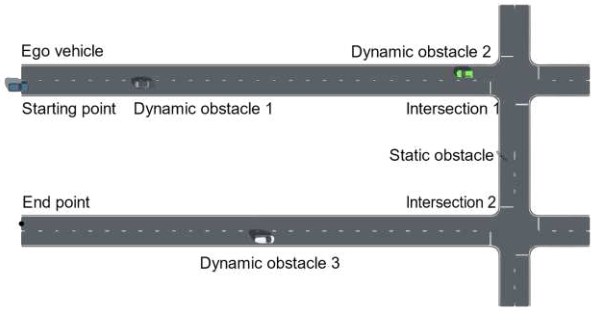


Fig.4 Simulation scenario

The time horizon T is 5s, and the time interval is 0.1s. The lane width is 3.5m. The wheelbase of ego autonomous vehicle is 2970mm. The initial speed of ego vehicle is 60km/h. The dynamic obstacle 1 is 30m ahead of ego vehicle, and driving east at constant speed 20km/h. The dynamic obstacle 2 is 105m ahead of ego vehicle, and driving west at constant speed 20km/h. The dynamic obstacle 3 is driving east at constant speed 20km/h. The ω_1, ω_2 and ω_3 are 0.5, 0.2 and 0.3 respectively.

4.2. Simulation results

We input the global route points' coordinates, road information, obstacles' predicted trajectory possibility distribution to the Matlab optimization tools to solve the problem (12), then use G^1 clothoid fitting method fit the predicted trajectory into clothoid curve and transfer to Prescan, the results is shown in Figure 5.

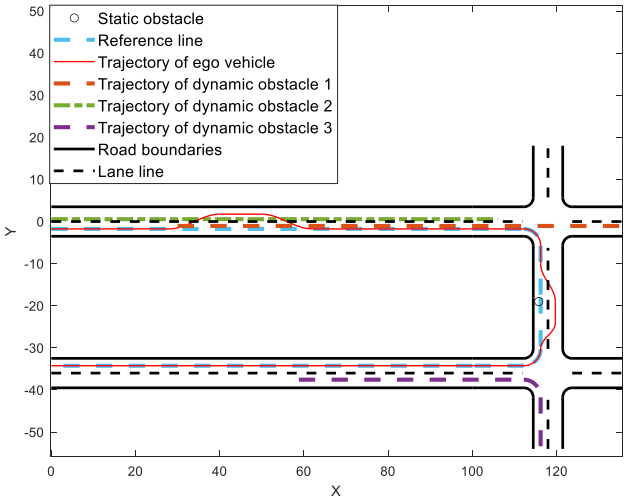


Fig.5 Simulation trajectory results

The trajectory predicted for the ego vehicle is collision-free and satisfy the requirements of vehicle dynamics.

5. Conclusions

The local trajectory planning method for autonomous vehicle based on dynamic programming designed in this article can satisfy both safety and vehicle dynamics requirements. This method has high accuracy and fast computing time, which can satisfy the requirements for application of autonomous vehicle driving on real roads. Future related works can consider testing in more complex scenarios and optimize the value of the weight parameters.

References

[1] Claussmann, L., Revilloud, M., Gruyer, D. and Glaser, S., "A review of motion planning for highway autonomous driving", IEEE Transactions on Intelligent Transportation Systems, 21(5), pp.1826-1848, May 2019.

[2] Claussmann, L., Carvalho, A. and Schildbach, G., "A path planner for autonomous driving on highways using a human mimicry approach with binary decision diagrams", 2015 European Control Conference (ECC), pp. 2976-2982, IEEE, July 2015.

[3] Gu, T., Snider, J., Dolan, J.M. and Lee, J.W., "Focused trajectory planning for autonomous on-road driving", 2013 IEEE Intelligent Vehicles Symposium (IV), pp. 547-552, IEEE, June 2013.

[4] Schubert, R., Scheunert, U. and Wanielik, G., "Planning feasible vehicle manoeuvres on highways", IET Intelligent Transport Systems, vol. 2, no. 3, pp. 211–218, Sep. 2008.

[5] Choi, Jiwung, "Kinodynamic motion planning for autonomous vehicles", International Journal of Advanced Robotic Systems, 11(6), p.90, June 2014.

[6] Bertolazzi, Enrico, and Marco Frego, "Fast and accurate clothoid fitting", arXiv preprint arXiv: 1209.0910, Sep. 2012.

[7] Bertolazzi, Enrico, and Marco Frego, "G1 fitting with clothoids", Mathematical Methods in the Applied Sciences, 38(5), pp. 881-897, March 2015.

[8] Kanchwala, Husain, Icaro Bezerra Viana, and Nabil Aouf, "Cooperative path-planning and tracking controller evaluation using vehicle models of varying complexities", Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science, p.0954406220945468, July 2020.

[9] Sheckells, Matthew, Timothy M. Caldwell, and Marin Kobilarov, "Fast approximate path coordinate motion primitives for autonomous driving", 2017 IEEE 56th Annual Conference on Decision and Control (CDC), pp. 837-842, IEEE, Dec. 2017.

[10] González, D., Pérez, J., Milanés, V. and Nashashibi, F., "A review of motion planning techniques for automated vehicles", IEEE Transactions on Intelligent Transportation Systems, 17(4), pp.1135-1145, Nov. 2015.

RESEARCH ON SECURITY ISSUES OF MILITARY INTERNET OF THINGS

LI XIANLI[1], PAN WEI[2], ZHANG JIAWEI[3], LIU GUOSONG[1], WAN PING[1]

[1]Military Logistics Department, Army Logistics University of PLA, Chongqing, China
[2]32366 troops of PLA, Beijing, China
[3]Chongqing Innoway Information Technology Co. Ltd, Chongqing, China
E-MAIL: lixianli1818@163.com, plapw@sina.com, 1805839946@qq.com

Abstract:

Military Internet of things is the application of Internet of things in the military field, after several years of development, the security problem of military Internet of things is becoming increasingly prominent. How to improve the network security is the key problem of military Internet of things. This paper analyzes the security threats of military Internet of things, and the countermeasures to improve the security of military Internet of things are put forward. The attacks on the military Internet of things will directly lead to the whole networks disabled or interruption of communication, the consequences are not measurable, so, it is significant to study secure issues of military Internet of things.

Keywords:

Military Internet of things; Security Threats; Network Attack; Terminal Equipment; Countermeasures

1. Introduction

Military Internet of things (MIOT) is the application of Internet of things technology in the military field, its connotation is very rich, and its contents and fields are very extensive. It mainly focuses on combat command, battlefield environment perception, intelligence reconnaissance, military training, warehousing logistics, medical support, intelligent barracks, fault diagnosis and other military applications. Military Internet of things is the evolution of the concept and technology of the Internet of things in the military fields, it is of all typical features of Internet of things.

With the development of mobile internet, artificial intelligence, big data and other technologies, more and more devices are connected to the internet, ranging from routers, switch, server, computer and other equipment, more and more military entities are connected to the Internet. The era of military Internet of things is coming, the technology of military Internet of things has been applied to many aspects, and its application will be more extensive and continue to grow in the future. Therefore, the security of military Internet of things is an important subject that must be paid attention to and studied.

What is the security issue of military Internet of things? the research on the information security of military Internet of things must be combined with the analysis of hierarchical structure and specific technology, in order to have an overall grasp and scientific understanding, we must put forward specific countermeasures and reduce the military risks it brings.

With the growth of number and scale of military Internet of things, it has gradually become an important factor restricting the overall development of military Internet of things, based on the architecture of military Internet of things, the organizational structure of the paper is as follows: firstly, this paper lists the main security threats faced by military Internet of things, the second part of the paper analyzes the security architecture of military Internet of things, and the third part puts forward the corresponding security measures, finally, the paper summarizes and prospects.

2. Security threats of Military Internet of Things

Military Internet of things is widely used in all kinds of aspects, such as smart camp, smart site, smart campus, intelligent transportation, intelligent medical treatment, and so on. In order to meet the needs of all kinds of military applications, there are many problems caused by the technology of military Internet of things, for example, there are many kinds of terminal equipment, which is of different sizes, forms and functions, and network connecting methods are different, such as wired, wireless, Bluetooth, Zigbee, third generation mobile communication, fourth generation mobile communication, fifth generation mobile communication, and so on, the data of military Internet of things stored in cloud platform is generated like a treasure trove of data, hackers are lured all the time. The attacks may

lead to the whole networks disabled and interruption of communication in each links of military Internet of things. The security threats of military Internet of things are shown in Figure 1 below, this paper mainly lists five kinds of security threats of military Internet of things.

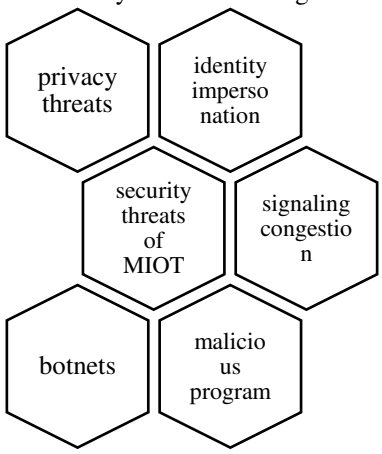


Fig.1 The security threats of MIOT

(1) Privacy threats. Wireless communication is the one of communication mode in military Internet of things, a large number of electronic tags and unattended equipment are used, due to the limitation of cost and performance, most of the terminals used in military Internet of things are weak terminals, it is easy to be illegally intruded or even destroyed, the attacker can obtain the military secrets, it brings potential safety hazard.

(2) Identity impersonation. Some management password settings of military Internet of things are too simple, there are some factory default passwords, these devices are hard to find in a short time after being hijacked. At this time, they can disguise as clients or servers to send data and perform some malicious operations. For example, access control system can be set easily, attackers can easily get in and out of the room.

(3) Signaling congestion. The authentication mode of terminals and servers in military Internet of things is ordinarily adopted as one-to-one, which leads to exist a large number of terminals in military Internet of things, when these terminals are exchanging data, they will make large-scale authentication requests to the server. At this time, this information will lead to server overload, which will cause congestion in the information channel of networks, and indirectly lead to DDoS attacks. For example, some data points out that under a DDoS attack on the Internet of things, a large area of the network in the eastern United states was paralyzed, and many well-known websites, including PayPal, Twitter, Spotify, Netflix, were unable to log in.

(4) Malicious program. Malware enters the wireless network and sensor network environment by many ways, once the intrusion is successful, its propagation, concealment and destructiveness are more difficult to prevent than TCP/IP network. For example, malicious code like worms does not need parasitic files, so it is very difficult to detect and remove such malicious code.

(5) Botnets. Botnet is a series of malware. Attackers spread zombies through various ways to infect a large number of hosts of networks, and perform a series of malicious activities, such as distributed denial of service attacks, sending spam. This kind of network attack can lead to the paralysis of basic network or important application system, it can also be used to engage in network fraud activities.

In July 2017, American vending machine supplier Avanti Markets was hacked into the intranet. The attacker implanted malicious software into the terminal payment device and stole personal information such as user credit card account and biometric data. In November 2017, Check Point researchers said that LG smart home device has a vulnerability, hackers can use this vulnerability to completely control a user account, and then remotely hijack LG smart devices. Green Alliance Technology pointed out in the 2018 Internet of things security annual report that attackers wrote malicious software to infect a large number of Internet of things devices, bought and sold attack services in dark network, and wantonly launched destruction and blackmail attacks. The security of military Internet of things is facing a severe challenge both international and domestic, many domestic and international organizations have put the military Internet of things security research on the agenda.

3. Security Analysis of Military Internet of Things

3.1. The Architecture of Military Internet of Things

Based on the properties of military Internet of things, the architecture of military Internet of things is generally divided into perception layer, network layer and application layer. The security architecture of military Internet of things is shown in Figure 2 below.

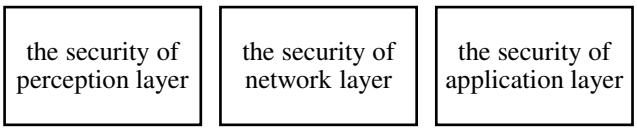


Fig.2 The security architecture of MIOT

The perception layer of military Internet of things collects information, and realizes the information acquisition and identification of objects, mainly through the front-end

control module, sensor module, camera, radio frequency identification module, positioning chip, laser scanner and other equipment. There are many manufacturers of these equipment, and they have different understanding to safety problems, and their capacity is different, so the degree of safety measures taken is also different. There are more vulnerabilities in the device itself, so attacks on the perception layer of military Internet of things will also be increasing. For example, the perception layer is vulnerable to physical attacks, forgery attacks, resource exhaustion attacks, privacy disclosure threats, etc.

The network layer of military Internet of things is to transmit the data of upper and lower layers efficiently, stably, timely and safely, and achieve the connection of things through the choice of communication mode, protocol development, and so on. It is a heterogeneous network, including the traditional computer network, communication network, radio network and a variety of emerging new access network and private military network, such as sensor network, car area network, special network. Therefore, the security problems of network layer include not only the security problems of traditional network in the past, but also the problems of new network. Such as the problem of heterogeneous network data exchange, due to the security weakness of network protocol and technology itself, it is vulnerable to asynchronous and collusive attacks. Due to a large number of network terminals and different defense capabilities of equipment, it is easier to launch distributed denial of service attacks, for the huge amount of data processing, the more the network data processing equipment required is, the more difficult the device management is, the more likely it is to suffer from various network attacks.

The application layer of military Internet of things carries the use of military Internet of things system, it is the purpose of the development of military Internet of things, especially due to the development of cloud computing, it provides users with rich applications in the cloud. The application layer includes service support layer and application subset layer. The service support layer is mainly composed of a large number of cloud computing platforms, information open platforms, data mining and analysis platforms and other groups. A large amount of data is stored in the application layer, so the confidentiality, integrity, availability of data and the stability of platform equipment exists security issues. In the application layer of military Internet of things, the operating system, platform components, service programs and so on, have their own vulnerabilities or design defects, which can easily lead to various attacks, such as unauthorized access attacks, open port attacks and so on.

3.2. Analysis from service providers of Military Internet of things

The product manufacturers of military Internet of things can be divided three aspects: software manufacturers, hardware equipment manufacturers, network service providers and users. The supply chain of military Internet of things is long, seriously fragmented, and the rate of product innovation is fast. Many military Internet of things equipment manufacturing enterprises only seek for quick and innovative products in the production process, without considering the safety issues or the safety issues are not considered perfectly. The products produced are easy to create security vulnerabilities, and once the security problems occur, the manufacturers also lack the corresponding safety mechanism. The service providers of networks are usually professional managers who can provide professional management capabilities of networks. However, there are still some problems in the management of a large number of bottom perception network, such as the absence of managers or the lack of management means or technology, the users of military Internet of things vary greatly. There are differences to the application ability of products of military Internet of things, many users lack professional knowledge and weak security awareness. For example, the setting of security password is quite weak, the products of military Internet of things are not upgraded, and there is no anti-virus. All of these can easily lead to potential safety hazards.

3.3. Analysis from military standard

From the current development of military Internet of things, there are many kinds of products of military Internet of things, and the products change rapidly. There is no unified technical standard and coordination mechanism in the Internet of things industry, and the enterprises basically act on their own affairs. Therefore, information security is bidding farewell to the traditional stages of virus infection, network hackers and resource abuse, and it is stepping into a new period of complex, diversified and comprehensive interaction.

4. Security Countermeasures of Military Internet of Things

4.1. Strengthen Identity Authentication

Identity authentication can effectively resist the threats of impersonation, illegal access and replay. For the applications of networks, most designers will adopt one-time authentication to pass through the entire network system

because of convenience, therefore, Reliable identification authentication is needed in the unified system access port. At the same time, in order to prevent the attacker from using some untrusted devices access to military Internet of things, such as routers controlled by attackers, we also require the use of devices authentication. Security issues can be resolved through the degree of password strength, dynamic and static password settings, verification input, non-public certificate, electronic Certificate and biometric technology, and so on, some key nodes need to be designed specifically.

4.2. Perfect encryption mechanism

Due to the close combination of network connection and business use in military Internet of things, it is necessary to encrypt the links that need to be protected. For some services that do not require high security requirements, the security mechanism can be transparent to the business, and hop by hop encryption can be used to implement security management of different services on the unified business platform of military Internet of things. But because hop by hop encryption needs to decrypt the data on each transmission node, each node may interpret the plaintext of the encrypted message. Therefore, for the business with high security requirements, end-to-end encryption and confidentiality measures can be adopted.

4.3. Purify network environment

Network environment is the basis of the normal operation of whole military Internet of things, from manufacturers to users we should pay close attention to their safety. Communication protocols often become a good breakthrough to attackers, therefore, manufacturers should do the adequate testing before opening applications, and timely update the vulnerability patch. At the same time, the safety inspection frequency of the system should be increased to reinforce the system, especially, botnets should be cleaned up in time to cope with the problem.

4.4. Realize multi-level defense

Through multi-level defense measures, strengthen access control, the security of military Internet of things is better safeguarded. Firewall is the first link between private network and public network, which can filter data and the access behavior of user. However, if the attacker uses signature detection to advance the attack, it must use user behavior analysis or security information management for defense in the next stage. Through big data analysis on the behaviors between users and equipment, it can analyze and monitor existing data, and predicts future threats.

Improve the professional level of military Internet of things related service providers, including the engineer of military Internet of things, the manager of military Internet of things, the equipment maintenance staffs of military Internet of things, the developers of military Internet of things, and so on. We must strengthen the safety awareness of military of things related enterprises and installation units, and carry out safety training for related persons of military Internet of things in different fields and links.

In order to ensure the equipment safety of military Internet of things, multi-party participation is full required. The general unit may not be able to bear the relevant expenses. Therefore, the relevant departments should support them through policies or funds to improve the enthusiasm of units to participate in safety design and safety research and development.

5. Conclusion

The rapid development of military Internet of things not only promotes technology progress, but also produces many problems. The security problem is one of them. With the development of military Internet of things, it is more and more important to strengthen the security of military Internet of things. At present, the development of military Internet of things is more emphasis on application than security, so it is necessary to improve the safety techniques and measures. In view of the current major security problems, we must formulate corresponding countermeasures, only if the security of military Internet of things is guaranteed, it can play a better role in promoting progress and development of military Internet of things.

References

[1] Su Yu. Research on the Internet of things security and privacy protection[J], Network security technology and application, No.1, pp.85-89, 2018.

[2] Zhou Ye, Yu Xiaosong. Research on security technology related issues of Internet of things[J]. China management informatization, Vol.20, No.4, pp.151-152, 2017.

[3] Wang Zhirui. On Internet of things security problems and related countermeasures[J]. Network security technology and application, Vol.4, No.3, pp.170-171, 2017.

[4] He Shengyong. Research on the security problems and solutions of the Internet of things[J]. Science and

technology communication, Vol.10, No.18 pp.102-103, 2018.
[5] Jia Yigang. The Application of Internet of things technology in environmental monitoring and early warning[J]. Shanghai construction technology, No.6 pp.65-67, 2010.

RESEARCH ON A SLIDING WINDOW BATS CODE METHOD

ZHUO YONGNING[1]*, ZHOU XIAOXUE[1], WANG QIN[1], ZOU ZONGZHENG[2], WANG SI[3], LIU YUN[4]

[1]National key laboratory of science and technology on communications, University of Electronic Science and Technology of China, Chengdu 611731, China; [2]School of Computer Science, Fudan University
[2]Shanghai 201203, China
[3]Shanghai Academy of Spaceflight Technology Beijing R&D Center, Beijing 100048, China
[4]The 54th Research Institute of China Electronics Technology Group Corporation, Beijing R&D Center, Beijing 100070，China
EMAIL: zyning@uestc.edu.cn, 17307130200@fudan.edu.cn, soleyoyo@sina.com, yunl_001@163.com

Abstract:

Aimed to realize reliable but time efficient data transmission in vulnerable space environment, an optimized sliding window transmission method based on BATS code (Batched Sparse Code) is proposed. In the scheme the unequal sliding step length of the window are used. While the small degree Batches are used to encode the data in the non-overlapping part of the window, the big degree Batches are used to encode the data in whole sliding window, and the probability distribution of the Batch degree is optimized through a heuristic algorithm. The results of the simulation experiment show that compared with the traditional successive sliding window, the transmission efficiency of our method is significantly improved, while the reliability is maintained at a similar level as the traditional method, hence the trade-off between the transmission reliability and time efficiency is improved.

Keywords:

BATS code; Fountain coding; Network coding; Sliding window; Space communication

1. Introduction

An ideal communication system is always expected to be both reliable and efficient, that is, to transmit messages with less resources and less errors in the same time, and as less as possible. But these two wishes are often contradictory in real environment. It is usual to use more resources (energy, frequency band, computing and memory resources, etc.) to ensure relatively high communication reliability. This issue becomes remarkable in the space communication, because the communication system's reliability in space is so important but the link is so vulnerable and the communication resources are usually rare. When a space communication system is in the design, its important parts, such as the modulation, encoding and decoding modules must be carefully evaluated.

BATS Code (Batched Sparse Code) is a new coding technique developed in recent years[1-2]. It is a combination of the fountain coding and the network coding. It not only possesses the benefits of fountain coding with little feedback message, but also possesses the advantages of network coding which can directly encode the received message in the intermediate nodes, which making it suitable for relay communication system [2]. As a contrast, the traditional fountain code must be decoded in intermediate node and then re-encoded to transmit, which introduces more transmission delay and system complexity. An experiment of ground video transmission has proved that [2-3], the system with finite length BATS code have better transmission fluency and reliability than the finite length fountain code in multi-relay transmission.

Although BATS codes show some excellent performance in multi-relay environment, its present research and application are still aimed at the data transmission on the earth's surface[4-5], which means that there is no need to concern about the energy and resources shortage. However, the extraterrestrial space is a more vulnerable environment. The space communication requires both high reliability and high transmission time efficiency. Usually, the redundant transmission of data packets through sliding window is used to ensure reliability[6-8], but the fast and time efficient transmission cannot be guaranteed in this way. Based on this, an optimized sliding window transmission scheme of BATS code is proposed in this paper. Compared with the common mode of successive overlapping sliding window [7-9], the window's sliding step length in our scheme for BATS code is variable, and the trade-off between the reliability and time

efficiency in transmission is improved.

2. Basic principle of bats code

2.1. The coding methods of BATS code

The batch processing is an important concept in the BATS code. Suppose the number of packets to be encoded is K, set B refers to the set of all packets, the collection is divided into n subsets (overlap is permitted), subset Bi⊂B, i=1,...,n. Corresponding to each set Bi, M encoded packets are obtained according to a matrix generalization of fountain code method, which is called a 'Batch'. The n Batches obtained after encoding are expressed as X1, X2,...,Xn, and each Batch can be expressed as (1) [1] :

$$\mathbf{X_i=B_iG_i} \quad (1)$$

where di = |Bi|, means Bi contains di original data packets, and di is called the degree of Batch Xi. Degree di, i=1, …, n, is independent identically distributed random variables, the distributionΨ= (Ψ1, …, Ψk) is called the Degree distribution, namely Pr{di= k}=Ψk. Gi is a random matrix of di×M, called a generative matrix. Theoretically, the number of encoded Batches n can be unlimited. The encoding and transmission process of BATS code is shown in figure 1. The dashed box besides the generated matrix Gi represents the generated Batch, and the solid square in the dashed box represents the M encoded packets in each Batch.

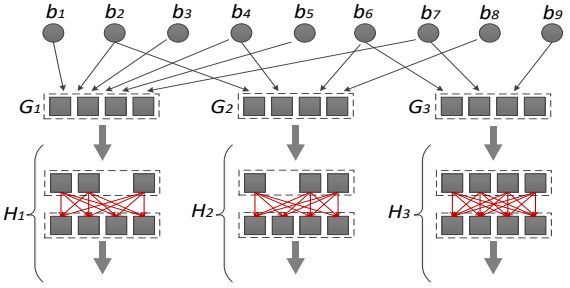


Fig.1 The encoding and transmission process of BATS code

When transmitting the data packets, the number of coded packets reaching the intermediate node in each Batch may be less than M due to the packet loss. The intermediate node uses the network coding for received packets in the same Batch to reproduce M coded packets and transmit to the next node. The ith Batch received in the final receiver can be expressed as (2).

$$\mathbf{Y_i=X_iH_i = B_iG_iH_i} \quad (2)$$

Where Hi refers to a random matrix with M rows called the transfer matrix. The columns **number** of Hi is equal to the number of the ith Batch's packet which reached the final receiver. The value may not be the same for different Batch, but it must be less than or equal to M.

2.2. The decoding method of BATS code

The common decoding method in BATS code is Belief Propagation (BP) decoding. After transmission, the information in the final receiver is Batch Yi, i=1,...,n, the transfer matrix H is included in the data packet header information, and the generation matrix G is obtained through the negotiation between the sender and the receiver. Therefore, the decoding information the decoder can use is (Yi , GiHi), i=1,...,n, and the decoding process can be regarded as the solution of linear equations. For a Batch, it's solvable when the rank of GH equals to the number of original packets used by the Batch (namely the degree of Batch). The corresponding raw packet is called the solvable packet. It's obvious that the less degree a Batch is with, the higher solvable probability the Batch will obtain.

The BP decoding contains multiple iterations. Every time the iteration happens, it selects a solvable packet and brings it to the connected and unsolvable Batch. The packet will be marked as solved after this and the unsolvable packet may become solvable, then the next iteration will begin. When there are no packets solvable, the decoding ends.

When the BP decoding cannot go on, we can decode the rest of the Batch by the Gaussian Elimination method, namely BP-GE algorithm [4].

3. The sliding window transmission of bats code

3.1. The analysis of traditional sliding window transmission method

Sliding window is a method used in streaming media transmission to improve reliability, which has been studied extensively in fountain code and RS code (Reed Solomon)[7-9]. The basic method is expressed in figure 2.

All data to be transmitted is divided into segments of length L which is called a window. After the data in a window are encoded and transmitted, the starting edge of the window is moved forward S symbols which is named as the sliding step S, then the data in the new window W2 are encoded and transmitted again. The overlap part of the front and back windows is shown in the figure 2 as P.

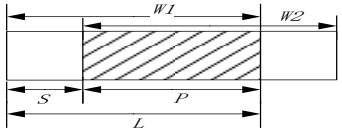


Fig.2 The basic sliding window transmission

Above method is a kind of overlapping sliding window, which realizes the enhanced protection for data in the overlapped parts by redundant transmission, and the reliability of data in this part is higher than that in non-overlapping part. If the window slides continuously, there will be more overlaps and the data protection levels of different overlaps are also different. For example, if the slide step S is less than the length of overlaps P, when the sliding keeps there may be triple or even more overlaps, which will leads to the overprotection for some data while little or no protection for other data. In the figure 3, data field P1 have no protection and P3 is overprotected.

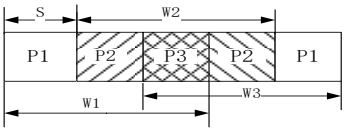


Fig.3 The overlapping field of a data section caused by consecutive sliding window transmission
P2: Double overlapped part P3:Triple overlapped part

3.2. The sliding window transmission method of BATS code with unequal sliding step

BATS code encodes data in Batches and the codes in different batches can be decoded jointly. As we know that Batches with smaller degree value has higher solvable probability. Based on this feature, a transmission method that evenly protects the overlapping and non-overlapping data in sliding window can be implemented. The procedure is as follows:

1) Firstly the sender obtains the BATS code's rank distribution based on the link condition and gets a expected value called rankexpt, then sets the size of every Batch M as rankexpt.

2) The sender sets a window length L, then determines the encoding rate and the number of coded packets every window needs to send by solving the evolutionary optimization in [1] according to the window length and rank distribution.

3) To form a Batch, a degree value d is randomly selected according to the Batch's degree distribution. If d < rankexpt, the d packets will be selected in the non-overlapping part of the window to form a subset Bi and form the codewords in the Batch. If d>rankexpt, the d packets will be selected randomly in the whole window to form the subset Bi and form the codewords in the Batch. The transmission for the current window will stop when the transmitted codewords reach the total codewords number determined in step 2).

4) Slide the window: when the transmission of current window finished, if the window has not overlapped with other windows yet, the window only slides sequentially with the pre-defined sliding step length. If this window has overlapped with other windows (which means it is already a sliding window), this window moves forward a full window length(select L new data as a new window) and start new sending process in steps 3 and 4 until the data sending finishes.

The data sending process is shown in figure 4. In the figure, The whole transmission process contain 4 windows, which are W1.,W2 , W3, W4 in turn. The data in area S1,S2,S3,S4 are randomly selected to form the Batches with small degree, and the data in every whole window Wi are selected to form the Batches with big degree. The sliding length between W1 and W2 is smaller than the one between W2 and W3 .

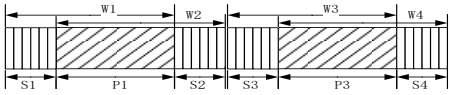


Fig.4 Sliding window transmission with balanced protection mode

3.3. Optimization of the Batch's degree distribution

From above analysis, we find that the data's transmitting efficiency and speed are depend on the Batch degree distribution. We take an example to analyze. Suppose the total number of packets is 1024, the window length wnd_len is 256, the communication links are independent multi-hop links with hops 2, the packet loss rate p is 0.2 per hop , M =16. The link topology is shown in figure 5.

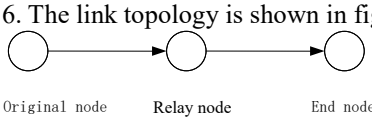


Fig.5 The Topology of multi-relay transmission

Using the Binomial Distribution fitting method, the rank distribution is obtained in figure 6, where the value of rankexpt is 12.87.

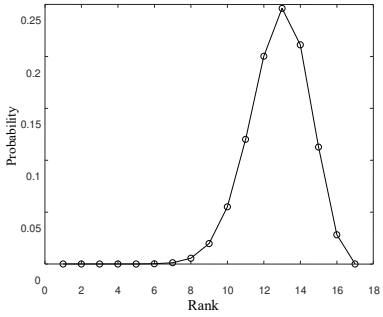


Fig.6 The distribution of rank of GH

Based on above rank distribution, by solving the optimization problem of code rate in [4], the degree distribution is obtained in figure 7.

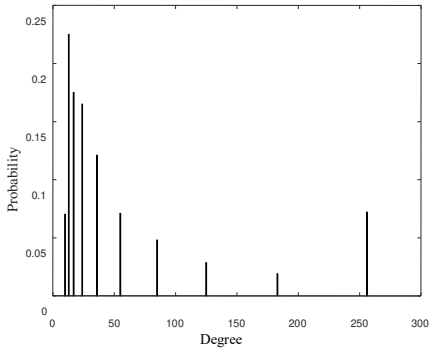


Fig.7 The distribution of Batch degree obtained by solving the optimization problem of [4]

According to above probability, the small degree value has relatively big probability. This will produce a large amount of Batches with small degree value, and cause the low sliding speed of the window. This situation may happen in the solving process of optimization problem in [4]. To prevent the low sliding speed, we need to adjust the small degree value and its probability. Hence we propose a heuristic algorithm of the degree distribution, which is based on greedy algorithm. The algorithm is described as follows:

Initialization:

Set value of loop_times // define the number of iterations

Set value of adjust_value // define the degree value distribution for each adjustment

Loop:

for i = 1:loop_times

calculate the decoding failure probability under given degree

if the decoding failure probability is within the acceptable range

1: randomly pick a degree greater than rankexpt from the degree distribution then minus adjust_value

2: randomly pick a degree smaller than rankexpt from the degree distribution adds adjust_value；

else

break；

end if

end for

The Batch's degree distribution which generated through this way is shown in figure 8. We can see that the probability of small degree value(less than 12) has been increased.

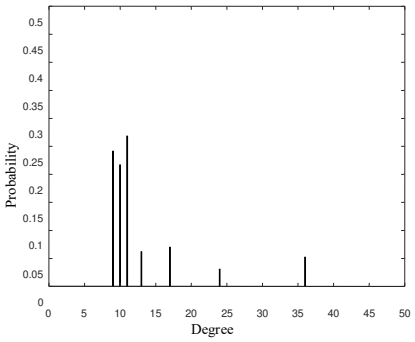


Fig.8 Adjusted distribution of Batch degree suitable to sliding window transmission

4. The simulation analysis

The specific simulation scenario is three-point two-hop link, and the packet loss rate is set in every hop in the efficiency simulation, which is variable in reliability simulation. The total number of source packets is 1024 and the link has no feedback. In order to compare the transmission performance between our method and other sliding window method, the following four schemes have been conducted:

1) Classic fountain code is adopted in the coding mode, namely LT code (Luby Transform). It uses finite code length and its decoding mode is GE (Gaussian Elimination)[4] algorithm. The original data is sent by segmenting coding in order (which means there is no overlap between segments). The segmenting length is 256 （Window Size =256 packets） and the length of each segment of coded packet is 480 (30 Batches for each window). This scheme simulates LT fountain code transmission without sliding window.

2) The coding mode is BATS code and the decoding mode is BP decoding algorithm. The size of the finite domain Fq=256. The original data is sent by segmenting coding in order and there is no overlap between segments. The size of Batch is M=16. The segmenting length is 256 and the length of each segment of coded packet is 480. The Batch degree distribution is like the degree distribution shown in figure 7. This scheme simulates BATS code transmission without sliding window.

3) The coding mode is BATS code and the decoding mode is BP decoding algorithm. The size of the finite domain Fq=256. The transmission scheme is sequential overlapping sliding mode (which is the sending mode in figure 3). The size of Batch M=16. The segmenting length is 256 and the length of each segment of coded packet is 480. This scheme simulates traditional BATS code transmission with successive sliding window.

4) The coding mode is BATS code and the decoding mode is BP decoding algorithm. The size of the finite domain Fq=256. The transmission scheme is balanced sliding mode proposed in this paper. The size of Batch M=16. The segmenting length is 256 and the length of each segment of coded packet is 480. The degree distribution is shown in figure 8. This scheme simulates BATS code transmission with the sliding window of un-equal sliding length proposed in this paper.

Figure 9 shows the percentage of successful recovered data varying with the number of encoded packets sent. The data recovery rate is defined as the ratio of the recovered data packets to the original data packets involved in the encoding procedure in each segment, and the sent rate is defined as the ratio of the coded data packets having been sent to all original data packets. We can see that the recovery rate of sliding window mode is higher than that of non-sliding window mode. When sending the same number of packets in non-sliding window mode, BATS coding have a higher successful recovery rate than LT code. When reaching the 100% recover rate, the LT code needs to send about 1.3 times amount of original packets, which is almost the same as the BATS code. In the two BATS code modes in sliding window mode, the recovery rate of unequal sliding length of sliding window is a little less than the successive sliding window, but it need less coded packets to send than the successive sliding window mode.

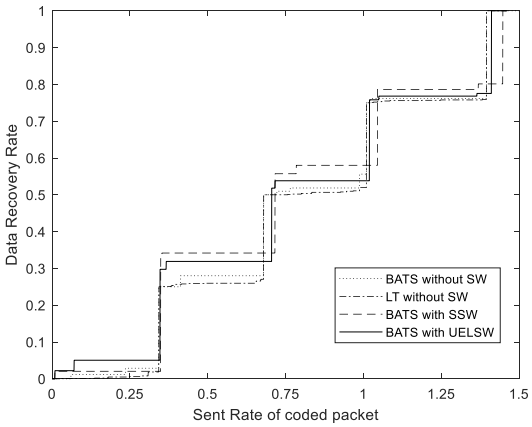


Fig 9. The data recovery rate for different transmission scheme

Figure 10 shows the successful data recovery rate in the case of different packet loss rates in channels. The number of coded packets sent is fixed at 2700 in the figure. The result can reflect the transmission reliability of each scheme. In the figure, when the packet loss rate in the link is less than 0.3, all the transmission methods can recover the data successfully, but when the packet loss rate is above 0.4, the successful recover rate of non-sliding window mode goes down to 0 quickly while sliding window mode still maintains at a high level. The successful recovery rate of successive sliding window(SSW) mode is slightly higher than the unequal length sliding window(UELSW) mode, which means although the reliability of UELSW mode is lower than the successive overlapping sliding window mode, but it still keeps at a relatively high level and can be used when the maximum packet loss rate reaches 0.4.

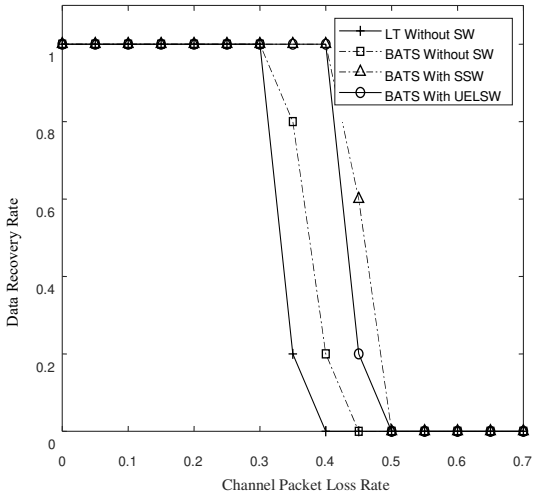


Fig.10 The data recovery rate at different packet loss rate in channel

5. Conclusion

In this paper, aimed to realize a reliable but time efficient transmission for important data in the vulnerable environment such as the telemetry/ telecontrol in space communication, an optimized transmission method for BATS code is proposed. The main characteristics in the method are:

1) A limited redundant transmission.

2) The different Batches degree are differently used in the encoding process. The Batches with small degree are used without redundancy, but the Batches with big degree value are partly repeated in the sliding window.

3) With above methods, high transmission reliability and efficiency can be achieved in the case of high packet loss rate in the vulnerable environment, and the trade-off of the transmission reliability and efficiency is improved. The simulation results show that the transmission efficiency of this scheme is significantly improved, while the reliability is maintained at a similar level with the traditional successive sliding window method.

Acknowledgements

The work in this paper is supported by the National Manned Space Flight research project 060501, and the 13th 5year research of civil space flight research project B0111.

References

[1] Yang S H, Yeung R W. Batched sparse code[J], IEEE Transaction on Information Theory,2014,60 (9) :5322-5345.

[2] Yeung R W, Dong G L, Zhu J, et al. Space communication and BATS codes: a marriage made in heaven [J]. Journal of deep space exploration,2018,5(2):129-139.

[3] The Institute of Network Coding, The Chinese University of Hong Kong, BATS code for network transmission [EB/OL]. 2016[2019]. http://www.inc.cuhk.edu.hk/research/bats.

[4] Yang S H, Tsz-Ching Ng, Yeung R W. Finite-length analysis of BATS codes[J]. IEEE Transactions on Information Theory,2018,64(1):322-348.

[5] Zhao H K, Yang S H, Feng G N. Fast degree-distribution optimization for BATS codes[J]. Science China(Information Sciences), 2017, 60(10):124-138.

[6] Zhao H K, Yang S H, Dong G L. A polynomial formula for finite-length BATS code performance[J].IEEE Communication Letters,2017,21(2):222-225.

[7] Mattia C O B, Pasquale C, Marco G, et al. Sliding-window digital fountain codes for streaming of multimedia contents[C]//IEEE International Symposium on Circuits and Systems, New Orleans,LA,USA:IEEE,2007:3467-3470

[8] Weng Y T, Shih C H, Chou Y K, Sliding-window forward error correction using Reed-Solomon code and unequal error protection for real-time streaming video[J], International Journal of Communication Systems,2018,31(1):1-18

[9] Cataldi P, Grangetto M, Tillo T, et al. Sliding-window raptor codes for efficient scalable wireless video broadcasting with unequal loss protection[J], IEEE Transaction on Image Processing, 2010,19(6):1491-1503

POTENTIALLY INVALID: STABLE MATCHING WITH OUTSIDE OPTION

LIAO JIE[1], SUN SHAOWEI[1]

[1] School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China
E-MAIL: liaoj@std.uestc.edu.cn, 201922080809@ std.uestc.edu.cn

Abstract:

Matching is based on the order of selection given by the participants. We found that in real life, there are indeed other ideas when matching. We want to reject the matching when there is no suitable object in the matching. We abstract all non-opposite choices as "outside option". This means that each applicant and the hospital have a total order of opposites and an "outside option". In this paper, we use virtual objects as "outside option" to implement extended deferred acceptance algorithm. The extended deferred acceptance algorithm does not destroy the original structure, and has proven to retain the same properties. In addition, we proved that when there are "outside option", potentially stable matches may have invalid matches.

Keywords:

Stable matching; DAA; Outside option

1. Introduction

Stable matching is a typical mechanism design for exchanging items to generate revenue. Stability means that there are no two market participants, and their interest in each other is greater than the current matching objects. Gale-Shapley algorithm (referred to as "GS algorithm", also known as "deferred acceptance algorithm ") is a market mechanism designed by Gale and Shapley, the purpose is to find a stable match. The deferred acceptance algorithm used to solve practical problems usually requires very little modification, and is often used for stable matching problems, such as employment allocation, dormitory allocation, housing allocation, courtship allocation, and school selection.

Now we need to extend the model definition and deferred acceptance algorithm to be able to adapt to the "outside option" between the application and the hospital. "Outside option" means any option other than application, acceptance. Applicants may only want to apply in one place, but have no interest in other hospitals; hospitals prefer local applicants, but only a small percentage are local applicants; applicants have a backup plan for graduation plans; hospitals are more willing to recruit not to apply People on the list. The contribution of this paper is to expand the model definition and deferred acceptance algorithm, and prove that the nature of the algorithm remains.

2. Algorithm Review

We review model definitions, algorithms and theorems.

2.1. The Model

- n represents the number of applicants / the number of hospitals, is a positive integer.
- V is a finite set, representing applicants, with n elements.
- W is a finite set, representing hospitals, with n elements.
- $V_{i-\text{order}}$ represents the set in which V_i preferentially sorts the elements in the W set, with the most preferred vertex on top. $i \in n$.
- $W_{i-\text{order}}$ represents the set in which W_i preferentially sorts the elements in the V set, with the most preferred vertex on top. $i \in n$.
- M represents the set of matching results. (V_i, W_i) represents the matching result, W_i accepts V_i. $i \in n$.
- Vertices $V_i \in V$ and $W_i \in W$ form *a blocking pair* for M if they are not matched in M, V_i prefers W_i to her match in M, and W_i prefers V_i to its match in M. A blocking pair spells trouble, because the two vertices are tempted to secede from the process and match with each other. A perfect matching is stable if it has no blocking pairs [1].

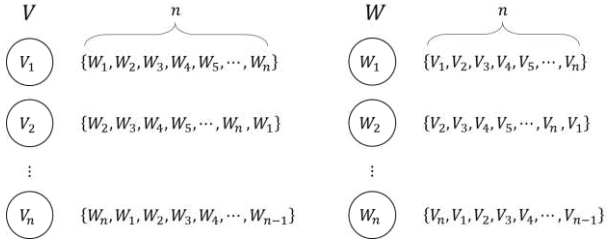


Fig.1 An instance of stable matching. Each vertex is annotated with its total ordering over the vertices of the opposite side, with the most preferred vertex on top.

2.2. The Deferred Acceptance Algorithm

Alg.1 Deferred Acceptance Algorithm

while there is an unmatched applicant $V_i \in V$ **do**
  V_i attempts to match with her favorite hospital W_i who has not rejected her yet
  if W_i is unmatched **then**
    V_i and W_i are tentatively matched
  else $\{W_i$ is tentatively matched to V_j and $i \neq j\}$
    W_i rejects whomever of V_i, V_j it likes less and is tentatively matched to the other one all tentative matches are made final
  end if
end while

2.3. Theorem

We note several properties of the deferred acceptance algorithm. First, each applicant systematically goes through her preference list, from top to bottom. Second, because a hospital only rejects an applicant in favor of a better one, the applicants to whom it is tentatively matched only improve over the course of the algorithm. Third, at all times, each applicant is matched to at most one hospital and each hospital is matched to at most one applicant.

3. Extend Algorithm

Each object has an "outside option", which has a different meaning, but the characteristic is that it does not want to choose either the applicant or the hospital. According to this feature, abstract options can be added for both sides for the other party to choose. In other words, the virtual object is added to the applicant and the hospital, the applicant also includes the virtual object in the ranking, and the hospital is also the same. Under the extended model, modify the deferred acceptance algorithm. First, it can only match W_{n+1} to fix this match. Second, skip comparing V_{n+1} first, and then compare after the match is completed. If the hospital prefers V_{n+1}, replace V_i with V_{n+1}. Third, delete matches that contain virtual objects.

3.1. Extend the definition

- n represents the number of applicants / the number of hospitals, is a positive integer.
- V' is a finite set representing applicants, where V'_{n+1} represents a virtual object, and the set has $n+1$ elements.
- W' is a finite set representing the hospital, where W'_{n+1} represents a virtual object, and the set has $n+1$ elements.
- $V'_{i-\text{order}}$ represents the set in which V'_i preferentially sorts the elements in the W' set, with the most preferred vertex on top. $i \in (n+1)$.
- $W'_{i-\text{order}}$ represents the set in which W'_i preferentially sorts the elements in the V' set, with the most preferred vertex on top. $i \in (n+1)$.
- M' represents the set of matching results. (V'_i, W'_i) represents the matching result, W'_i accepts V'_i. $i \in (n+1)$.
- $V'_{n+1-\text{order}}$ and $W'_{n+1-\text{order}}$ are empty.
- Vertices $V'_i \in V'$ and $W'_i \in W'$ form *a blocking pair* for M' if they are not matched in M', V'_i prefers W'_i to her match in M', and W'_i prefers V'_i to its match in M'.

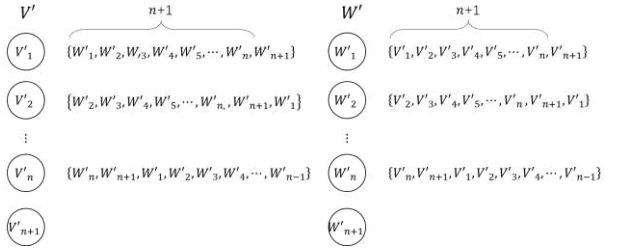


Fig.2 An instance of extend stable matching with an "outside option". Each vertex is annotated with its total ordering over the vertices of the opposite side, with the most preferred vertex on top.

3.2. Extend the DAA

Algorithm.2 uses code to describe the extend algorithm.

Alg.2 DAA with outside option

while there is an unmatched applicant $V'_i \in V'$ **do**
  if V'_i attempts to match with her favorite hospital W'_{n+1} **then**
    V'_i and W'_{n+1} are matched
  end if
    V'_i attempts to match with her favorite hospital W'_i, $i \neq n+1$ who has not rejected her yet
  if W'_i, $i \neq n+1$ is unmatched **then**
    V'_i and W'_i are tentatively matched
  else $\{W'_i$ is tentatively matched to V'_j and $i \neq j\}$
    W'_i rejects whomever of V'_i, V'_j it likes less and is tentatively matched to the other one all tentative matches are made final. Skip comparison with V'_{n+1}
  end if
end while
if (V'_i, W'_i), W'_i it likes V'_{n+1} more than V'_i **then**
  V'_{n+1} and W'_i are matched
end if
if Matching pairs in M' set contain V'_{n+1} and W'_{n+1} elements **then**
  delete these matching pairs from M'
end if

3.3. Extend theorem

The deferred acceptance algorithm still has several previous properties. First, each applicant systematically goes through her preference list $V'_{i-order}$, from top to bottom. Second, because a hospital only rejects an applicant in favor of a better one, the applicants to whom it is tentatively matched only improve over the course of the algorithm. Third, at all times, each applicant is matched to at most one hospital and each hospital is matched to at most one applicant. We note a new property. Fourth, the applicant do not match the hospital, and the hospital do not match the applicant. This does not contradict the third.

4. Experiment

Consider the instance in Figure.3. Suppose in the first iteration we choose the applicant V'_1, who tries to match with her first choice, W'_1. The hospital W'_1 accepts because it currently has no other offers. If we pick the applicant V'_2 in the next iteration, she also proposes to the hospital W'_1. Since hospital W'_1 prefers V'_2 to V'_1, it rejects V'_1 in favor of V'_2. If we pick applicant V'_3 next,

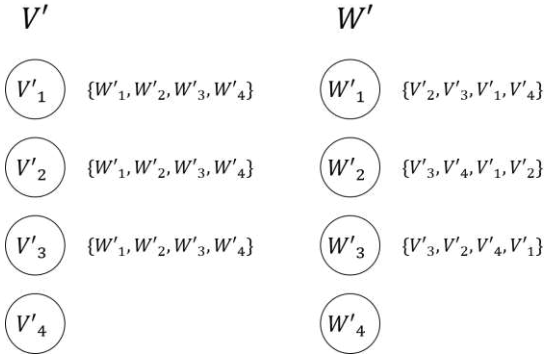


Fig.3 An instance of extend stable matching with $n = 3$. When $n = 3.$, V'_{n+1} is V'_4, and W'_{n+1} is W'_4.

the result is similar: W'_1 rejects V'_3 in favor of V'_2.

A possible trajectory for the rest of the algorithm is: applicant V'_1 now proposes to her second choice, W'_2; applicant V'_3 then also proposes to W'_2, causing W'_2 to reject V'_1 in favor of V'_3; and then, V'_1 proposes to her third choice W'_3, who accepts.

Now M = (V'_2, W'_1), (V'_3, W'_2), (V'_1, W'_3). (V'_2, W'_1), W'_1 it likes V'_4 less than V'_2, matching remains unchanged. Similarly, (V'_3, W'_2) remains unchanged. However, (V'_1, W'_3) it likes V'_4 more than V'_1. (V'_4, W'_3) replaces (V'_1, W'_3). Eventually, (V'_4, W'_3) is a Invalid match.

4. Conclusions

After expansion, it shows that if there is an "outside option", then some potential matches are invalid. In the future, it can also be applied to the exchange of commodities at the same price, even if someone only wants to sell their own things, they can also participate in the exchange.

Acknowledgements

Thanks to Wei Zukuan for their guidance. Thanks to the School of Computer Science and Engineering for providing the postgraduate exchange month platform.

References

[1] Strange H . Twenty lectures on algorithmic game theory.[J]. Computing Reviews, 2017, 58(10):581-581.

AN ANTI-INTERFERENCE ALGORITHM BASED ON ANTENNA ARRAY FOR VEHICLE NAVIGATION

YE QUANGUO[1,2], JI JING[3], CHEN WEI[2]

[1]Air Force Early Warning Academy, Wuhan 430019, China
[2] School of Automation, Wuhan University of Technology, Wuhan 430070, China
[3] School of Information Engineering, Wuhan University of Technology, Wuhan 430070, China
E-MAIL: yqg_200801@163.com, jijingisme@whut.edu.cn

Abstract:

Global Navigation Satellite System (GNSS), is a critical infrastructure that traffic users highly rely on. For the security risks caused by the low-cost jammer, this paper proposes an improved algorithm of the optimal weight coefficient base on the multi-antenna arrays. Via the simulation and field testing, it shows that our proposed has excellent anti-interference performance, and the probability of missed detection and false detection of the prototype is 40.073% and 8.0146% respectively. This work has great significance to the research and development of single-frequency anti-jamming, high-precision, real-time vehicle-based GNSS receivers in the future.

Keywords:

GNSS; Beidou; Anti-interference; Vehicle; Subspace constraints

1. Introduction

Global navigation satellite system (GNSS), currently includes four major systems: global position system (GPS), GLONASS, Beidou system (BDS) and Galileo. my country's Beidou-3 has started its global service in July 2020. According to public information [1], it can provide services with a global positioning accuracy better than 10 meters and a positioning accuracy better than 5 meters in the Asia-Pacific region. With the continuous development of major satellite navigation systems, GNSS has provided full-time and all-weather spatial information services for billions of users around the world. It has become a key infrastructure that countries rely on. However, in recent years, due to the GNSS itself vulnerability, complex electromagnetic environment and interference constitute a challenge to huge user terminals.

Vehicle users are the largest user group in traffic. At present, the user terminal of satellite navigation system has become a standard configuration of vehicles. Interference will pose a direct or indirect threat to this huge group, surrounding facilities and passersby. Therefore, the research on anti-jamming technology for vehicle navigation, namely algorithm research, has important research significance and great application value.

The interference against GNSS signals mainly includes suppression interference and deception interference. Suppressing interference usually involves using jammers to transmit interference signals to obscure the working spectrum of satellite navigation signals, so that user receivers reduce or even completely lose their normal working ability; deception interference is interference in the pseudo-range measurement and navigation positioning links of navigation receivers. It is divided into repeating interference that increases signal propagation delay and production interference that provides false navigation information [2-3].

At present, the methods of anti-interference mainly include: on-board anti-interference, receiver anti-interference and auxiliary anti-interference. The anti-jamming technology on the satellite is mainly to optimize the satellite, change the satellite orbit, increase the signal transmission power of the satellite load, enhance the service frequency of the satellite signal, and even optimize the design of the signal system [4-6]; receiver anti-jamming technology, realize the detection and suppression of interference in parts including antenna, intermediate frequency signal processing and digital signal processing. The main research hotspot of GNSS anti-jamming lies in this [7-9]; auxiliary anti-jamming technology is assisted by other means to complete the positioning and navigation function, common auxiliary technologies include integrated navigation, loran-C and radar, etc., there are the main directions of positioning, navigation and timing systems (PNTs) research [10-12], and are also a major research hotspot.

Because spatial filtering (also called beamforming) can distinguish interference and useful signals spatially, and deal with broadband interference and multiple narrowband

interference, it is widely used in antenna arrays. Zoltowski and Moleker of Purdue University first proposed the GNSS anti-jamming technology based on the power inversion (PI) algorithm. It does not need to know any prior information, is simple to implement, and has good effects, but it limits the number of interference sources. The array gain of the GNSS signal cannot be guaranteed [13-15]. Aiming at the problem that the gain of the satellite signal array cannot be guaranteed, Zoltowski proposes to use the minimum variance distortion response (MVDR) algorithm for GNSS anti-jamming, but the disadvantage is that the direction and elevation angle of each GNSS signal must be known in advance [16-18].

The organization of this paper as follows. Section 1 briefly introduces the current status of GNSS. Section 2 mainly describes the interference signal and introduces the antenna array model, then base on the linearly constrained minimum variance(LCMV) beamforming, proposes an improved algorithm for the optimal weight coefficient with subspace constraints. In section 3, the design of the experiment is listed at the first, then perform during the simulation and the field testing, and analysis to the result. In the rest, summarize and look forwards.

2. Models and Algorithm

Vehicle users are susceptible to interference from space-based, space-based, ground, and unknown interference sources during driving. As shown in Figure 1, these different types of interference will enter the receiver together with the GNSS signal for processing. Once the interference is the signal source identified as a GNSS satellite will cause a huge safety hazard to the safety of assisted driving and even autonomous driving vehicles.

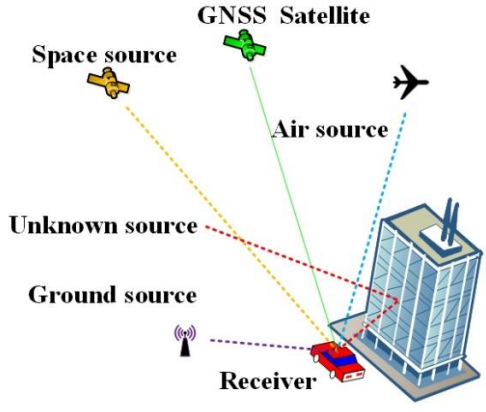


Fig.1 Schematic diagram of signal receives

2.1. Signal Model

Vehicle users are susceptible to interference from space-based, space-based, ground, and unknown interference sources during driving. As shown in Figure 1, these different types of interference will enter the receiver together with the GNSS signal for processing. Once the interference is the signal source identified as a GNSS satellite will cause a huge safety hazard to the safety of assisted driving and even autonomous driving vehicles.

It is assumed that the overall signal received by the user receiver is composed of three terms: GNSS useful signal, interference signal and thermal noise. Therefore, the vector form of the GNSS receiver signal is [19]:

$$\vec{s}(t)=\vec{s_d}(t)+\vec{s_i}(t)+\vec{s_n}(t) \tag{1}$$

where $\vec{s_d}(t)$, $\vec{s_i}(t)$ and $\vec{s_n}(t)$ are the vector forms of GNSS direct signal, interference signal and thermal noise during propagation. As shown in Figure 2, the composition of the received signal follows the vector sum rule. It is especially necessary to explain here that the propagation of the thermal noise vector is a random variable.

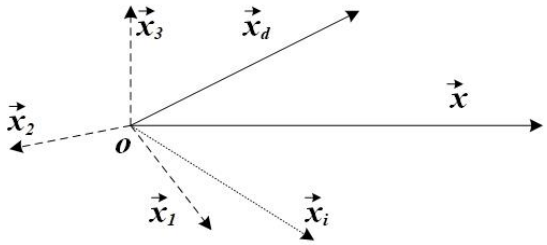


Fig. 2 Received signal composition

For the direct signal term in (1), it can be expressed as:

$$\vec{s_d}(t)=A_0 c(t-\tau_0)e^{-j\phi_0}e^{j\omega_c\tau_0} \tag{2}$$

where A_0 is the amplitude of the direct signal, $c(t)$ is the complex envelope signal transmitted by the GNSS payload, τ_0 and ϕ_0 are the propagation delay and carrier phase of the direct signal, and ω_c is the carrier angular frequency of the signal.

For the interference signal term, it can be expressed as:

$$\vec{s_i}(t)=\sum_{m=1}^{M}A_m c(t-\tau_m)e^{-j\phi_m}e^{j\omega_m\tau_m} \tag{3}$$

where A_m is the amplitude of the m-th interference, τ_m is the propagation delay of the m-th interference, ϕ_m is the carrier phase of the m-th interference, and ω_m is angular frequency of the m-th interference.

For the thermal noise term generated in propagation, it is regarded as a random variable with distribution as

$\overline{s_n}(t) \sim N(0, \sigma^2)$.

Take formula (2) and (3) into formula (1), there are:

$$\begin{aligned}\vec{s}(t) &= A_0 c(t-\tau_0) e^{-j\phi_0} e^{j\omega_c \tau_0} \\ &+ \sum_{m=1}^{M} A_m c(t-\tau_m) e^{-j\phi_m} e^{j\omega_m \tau_m} \\ &= A_0 c(t-\tau_0) e^{-j\phi_0} e^{j\omega_c \tau_0} \\ &+ \sum_{m=1}^{M} \alpha_m A_0 c(t-\tau_0-\Delta\tau_m) \cdot e^{-j(\phi_0+\Delta\phi_m)} e^{j(\omega_c+\Delta\omega_m)(\tau_0+\Delta\tau_m)}\end{aligned} \tag{4}$$

where α_m , $\Delta\tau_m$, $\Delta\phi_m$ and $\Delta\omega_m$ are the amplitude coefficients, propagation delay difference, phase difference and carrier angular frequency difference between the m-th interference and the direct signal, respectively. If $0 \le \alpha_m \le 1$, $\Delta\tau_m > 0$ and $\Delta\phi_m > 0$, the type of interference includes multipath effects and repeating interference caused by changes in environmental reflections; and the value $\Delta\omega_m$ is larger, it is usually the frequency offset caused by the receiver moving faster relative to the satellite. For ordinary vehicle receivers, the frequency offset is negligible.

However, the receiver can obtain the target signal by tracking the amplitude coefficient, relative delay difference and phase difference. Similarly, the waveform distortion-free algorithm can be used to achieve interference cancellation.

2.2. Smart Antenna Arrays

The smart antenna array, it can be called an adaptive antenna array, is the front end of the GNSS receiver model. Usually, according to the arrangement structure, the antenna array can be divided into hemispherical array, circular array, area array and linear array. The antenna array is adjusted by the algorithm so that the main lobe of the antenna's receiving beam points to desired signals or signals in the required direction and passes through zero. The signal in the interference direction is suppressed to the greatest extent, thereby improving the credibility of the received signal and the signal-to-interference-noise ratio (SINR). Thus, the smart antenna array mainly adopts beamforming technology, so that the received "purified" signal can effectively provide the correct pseudo-range or carrier phase.

Assuming that the smart antenna array is composed of N homogenous elements separated by d, the signals received by each element are adjusted by the adaptive processing module with M-level to obtain a weight matrix that matches the N-channel element, as shown in Figure 4.

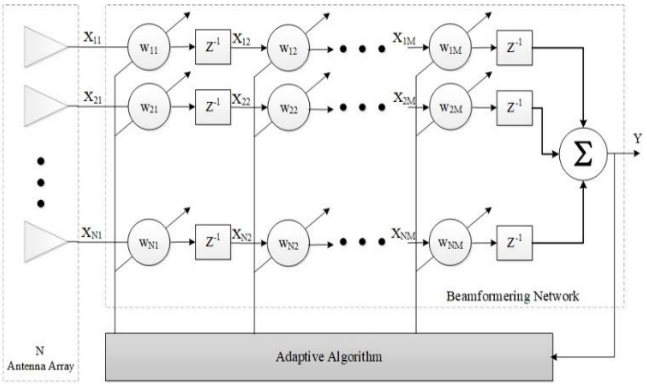


Fig.3 Smart antennas model

Assuming that the incident direction angle of the direct signal is and the elevation angle is, the final combined output can be expressed as [20]:

$$y_n(\theta, \phi) = \overline{W}^H \cdot \overline{X}(n) \tag{5}$$

where $\overline{W}$ is the weight coefficient vector, $[\cdot]^H$ is the conjugate operator, and $\overline{X}$ is the signal vector received by the *n*-th antenna array.

Take formula (1) into formula (5), that is:

$$X(t) = AS(t) + \xi(t) \tag{6}$$

where $A = [\alpha(\theta_1), \cdots, \alpha(\theta_N)]$ is the N array steering vector matrix, $\alpha(\theta_n)$ is the steering vector of the n-th source, $S(t) = [S_1(t), \cdots, S_N(t)]^T$ is the column vector of the complex envelope signal vector received by the N array element, , $S_n(t)$ is the composition envelope of the n-th source, and $\xi(t) = [\xi_1(t), \cdots, \xi_N(t)]^T$ is the column vector of the interference-noise terms vector received by the *N* element array, $\alpha(\theta_n) = [1, e^{j\beta_n}, \cdots, e^{(N-1)j\beta_n}]$, $(n = 1, 2, \cdots, N)$, and $\beta_n = \frac{2\pi}{\lambda} d \sin\theta_n$.

The autocorrelation matrix of the array signal is defined as:

$$\begin{aligned}R_{XX} &= E[X(t) X^H(t)] \sqrt{a^2 + b^2} \\ &= AE[S(t) S^H(t)] A^H + E[\xi\xi^H] \\ &= AR_{SS} A^H + \sigma_\xi^2 I_{\xi\times\xi}\end{aligned} \tag{7}$$

where R_{ss} is the autocorrelation matrix of desired signal, σ_ξ^2 is the variance of interference-noise term, and $I_{\xi\times\xi}$ denote the unit matrix with the interference-noise term.

The weight coefficient matrix can be expressed as:

$$W = [W_1, \cdots, W_N] \tag{8}$$

Thus, after weighting, the combined output power of

the array signal can be obtained as:

$$\begin{aligned} P &= E\left[\left|y(n)\right|^2\right] \\ &= E\left[\left(W^H X(n)\right)\left(W^H X(n)\right)^*\right] \\ &= E\left[W^H R_{XX} W\right] \end{aligned} \tag{9}$$

2.3. Optimal coefficient algorithm

Based on the constraints of PI algorithm, since GNSS interference is generally stronger than satellite signals and thermal noise, from the perspective of subspace, distinguish the interference subspace and the noise-added signal subspace, and separate them in the constraints The interference subspace and the signal plus noise subspace are correspondingly constrained, so that it can show better anti-interference performance no matter in the environment of strong interference or weak interference.

Assuming the noise-added signal power is σ_{S+N}^2, there are *N* interferences, and the interference power is σ_I^2, decomposition on the array received signal covariance matrix R_{xx}:

$$R_{xx} = \sum_{n=1}^{N} \lambda_n \Phi_n \Phi_n^H = V \Lambda V^H \tag{10}$$

where λ_n denotes the *n*-th eigenvalue of R_{xx}, $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_M > \lambda_{M+1} = \cdots = \lambda_{N+1} = \sigma_{S+N}^2$, Φ_n is the feature vector corresponding to λ_n. Λ is the diagonal matrix of eigenvalues, it can be expressed as:

$$\Lambda = diag\left[\lambda_1, \lambda_2, \cdots, \lambda_N\right] \tag{11}$$

V is a matrix composed of eigenvectors, it can be expressed as:

$$V = \left[\Phi_1, \Phi_2, \cdots, \Phi_N\right] \tag{12}$$

Assuming that there are eigenvector matrices corresponding to M eigenvectors, the interference subspace can be expressed as:

$$V_I = \left[\Phi_1, \Phi_2, \cdots, \Phi_M\right] \tag{13}$$

The noise-added signal eigenvector matrix corresponding to the remaining N-M features, subspace of the signal with noise-added, can be expressed as:

$$V_{S+N} = \left[\Phi_{M+1}, \Phi_{M+2}, \cdots, \Phi_N\right] \tag{14}$$

LCMV beamforming conditions are:

$$\varpi^H V_I = f_I \quad AND \quad \varpi^H V_{S+N} = f_{S+N} \tag{15}$$

where $f_I = \left[0, 0, \cdots, 0\right]$ is a $1 \times M$ dimensional constraint response vector, to ensure interference suppression for restricts the interference subspace. Each element of f_{S+N} can be 0, 1, or -1, but not all 0, which is a $1 \times (N-M)$ dimensional constraint response vector, and noise subspace constraints are added to the signal to ensure signal and noise reception. Among them, the number of 1 and -1 in f_{S+N} should be kept equal as much as possible to further cancel the residual interference in the signal plus noise subspace. The constraint conditions of formula (15) can be written together.

$$\omega^H \left[V_I, V_{S+N}\right] = \left[f_I, f_{S+N}\right] \tag{16}$$

Take $V = \left[V_I, V_{S+N}\right]$ into formula (16), that is

$$\omega^H V = \left[f_I, f_{S+N}\right] \tag{17}$$

Thus, the optimal weight coefficient can be expressed.

$$\omega_{opt} = R_{xx}^{-1} V \left(V^H R_{xx}^{-1} V\right)^{-1} f^H \tag{18}$$

Due to $VV^H = I$, I is the unit matrix with $N \times N$-dimension. Thus, the optimal weight coefficient is given by,

$$\omega_{opt} = Vf = V_{S+N} f_{S+N} \tag{19}$$

3. Test and analysis

3.1. Test design

This work described in this paper focuses on algorithms and some performance evaluation results. The experimental design flow chart of the work [21]is shown in Figure 5.

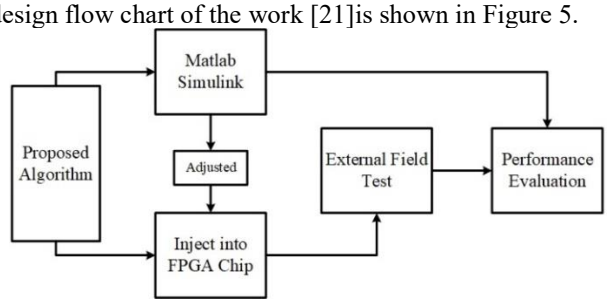


Fig.4 The flow chart of the test

The algorithm is simulated by software for anti-jamming, and the algorithm is adjusted and written into the field programmable gate array (FPGA), and testing the anti-jamming performance and the field location respectively.

The signal used in the simulation environment is the third-generation B1C signal of BDS-3, the carrier frequency *f* = 1575.42 MHz, the working bandwidth is 32.736 MHz, and the wavelength is = 0.19 m. The signal-to-noise ratio of the signal reaching the antenna section is about -28 dB, and the spreading code rate is 1.023 MHz. The sampling rate is 1 MHz. In most satellite navigation interference environments, the array model uses a typical 8-array circular array. The

distance between the array elements is 1/2 of the carrier signal wavelength, that is, d=0.095 m. The interference of broadband gaussian interference, the bandwidth is 1.023 MHz, and the center frequency is the same as the signal. The maximum number of interferences that must be limited in the experimental simulation is 7. The simulation diagram is shown in figure 5. The red dots in the figure are the interference sources, the green dots are the signal sources. And parameters settings are shown in table 1.

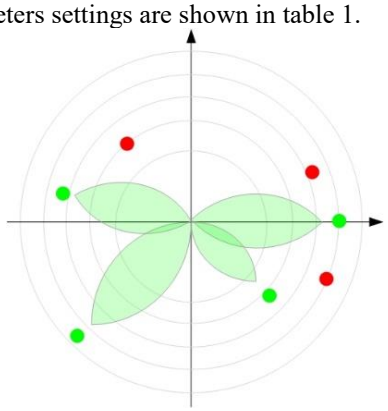


Fig.5 Simulation diagram

Table 1 Simulation parameters detail

Parameters	Details
The incident azimuth of the satellite signal / θ	-10°
Signal Noise Ratio	-20 dB
Interferences-1 type	Narrowband
No. of interference-1	4
Carrier frequency f	1575.42 MHz
The incident azimuths θ	Randomly generated
Interferences-2 type	Broadband
Bandwidth / BW	[f_d-BW/2, f_d+BW/2]
The incident azimuth θ_{i2}	70°
Interference Noise Ratio	10 dB
Sampling / L	2048

3.2. Simulation

The pattern of algorithms as shown in figure 6, our proposed has a deeper attenuation in the narrowband interference directions marked by dot line, compared with PI, and the algorithm forms the main lobe to the direction of the satellite signal marked by "+". For the broadband interference, although the proposed algorithm does not form null steering in the asterisk mark, it is still better than the classic PI in terms of mitigation effect.

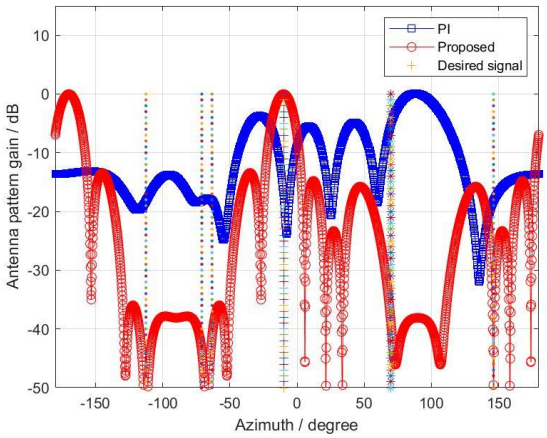


Fig.6 Pattern of algorithms

The algorithm injects into the FPGA chip to form a prototype, and install it on the vehicle to carry out an on-board test on an outfield section. The positioning effect of the algorithm is shown in figure 7. It should be noted that the position data is collected every 1 second, the sampling point of the location is 1000, which can be trimmed from the figure. The interference source has an obvious impact on the positioning, which will cause a great risk to the safety of the vehicle. The algorithm shown by the orange solid line can reduce interference influence in real-time.

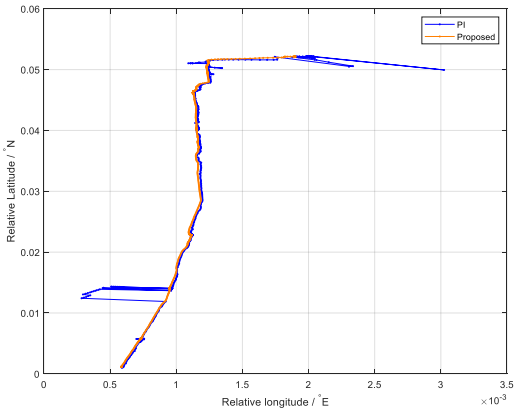


Fig.7 Algorithm-based location comparison

The interference source is fixed to ranges of the road section, and the field-testing location as shown in figure 8. The black dot indicates the sample when the antenna arrays receives the interference signal, and the red circle indicates the samples when antenna arrays detected and corrected.

The statistical results of the algorithm on the GNSS positioning performance are shown in table 2. In particular, the term missed detection means that there is interference in the environment of the vehicle antenna array but the

algorithm cannot be excited, and the term false detection refers to the environment of the vehicle antenna array. There is no interference but the algorithm implements processing.

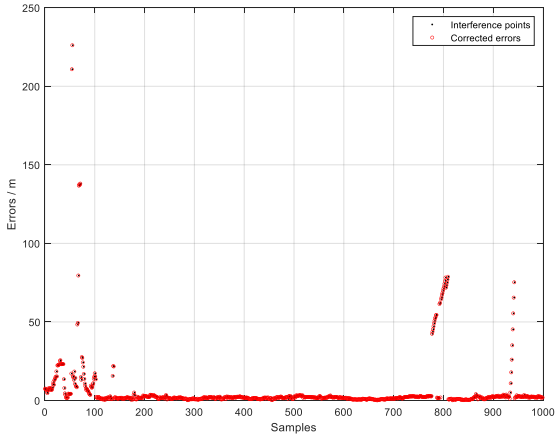


Fig.8 Performance of proposed in the field testing

Table 2 Field testing result

Performance	Details
Miss detection	40.073%
Fault detection	8.0146 %
No. of samples	329

Intuitively, the result value of the above indicators is not only related to the threshold of the algorithm, but also related to the hardware model and parameters of the antenna array.

4. Conclusions

This paper proposes an improved algorithm for optimal weight coefficients based on subspace constraints, and test the performance. It is found that there has significantly better anti-jamming performance than the classic algorithm, especially, the prototype's probability of missed detection and false detection can reach 40.073% and 8.0146%, respectively. Further, it still has potential as two aspects:

(1) To reduce the probability of missed detection and false detection further, from the study the relationship among the interference type, parameters, the hardware model and the algorithm threshold parameters.

(2) Due to the GNSS antenna array, the geometric shape among the elements is stable. This is a priori information that can be used to correct the position calculated by the receiver.

Acknowledgements

The authors are especially grateful for the prototype provided by Broadgnss Technologies Co., Ltd., and for the test equipment and vehicles provided by CTTIC.

References

[1] China Satellite Navigation Office. China Successfully Launched the 52nd and 53rd BDS Satellites. Accessed: Feb. 19, 2020. [Online]. Available: http://en.beidou.gov.cn/WHATSNEWS/201912/t20191216_19691.html

[2] Bauernfeind, Roland, et al. "Analysis, Detection and Mitigation of InCar GNSS Jammer Interference in Intelligent Transport Systems." Dlrk 2012.

[3] Hwang, Suk Seung, and J. J. Shynk. "Multicomponent receiver architectures for GPS interference suppression." IEEE Transactions on Aerospace & Electronic Systems Vol 42, No.2, pp. 489-502, Feb.2006.

[4] Hong-Hua, Liu, C. Qiao-Xia, and L. You-Xing. "Current Situation and Development of Anti-jamming Technology of GNSS." Shipboard Electronic Countermeasure, pp. , June.2014.

[5] Dempster, Andrew G., and E. Cetin. "Interference Localization for Satellite Navigation Systems." Proceedings of the IEEE, pp.1318-1326. 2016.

[6] Mao Hu, Wu De-wei and Lu Hu. "Analysis of Anti-Jamming Performance to GNSS Navigation Signals Design. "Journal of University of Electronic Science and Technology of China, Vol 7, No.4, pp.575-583.

[7] Wu, J., Huang, L., Tang, X., Li, B., & Wang, F.. "Distortionless Blind Beamformer for Interference Suppression in GNSS Antenna Array Receiver". Proceeding of China Satellite Navigation Conference (CSNC) 2020, Chendu, Vol 652. pp.733-741, June 2020.

[8] Zheng, Z., Li, M. Y., & Wang, W. J. "A high efficient baseband gnss signal narrow band anti-jamming approach in frequency domain. " Advanced Materials Research, pp.926-930 & pp.1857-1860. 2014.

[9] Chuang-Liang Chang, Bo-Han Wu. "Analysis of performance and implementation complexity of array processing in anti-jamming gnss receivers. "Electrical & Electronic Engineering, Vol 1, No.2, pp.79-84. 2011.

[10] Ziebold, R., Dai, Z., Lanca, L., Noack, T., & Engler, E.. (2013). Initial realization of a sensor fusion based onboard maritime integrated pnt unit. Transnav International Journal on Marine Navigation & Safety of Sea Transportation, 7(1), 127-134.

[11] Schutz, A., Sanchez-Morales, D. E., & Pany, T.. (2020). Precise positioning through a loosely-coupled sensor fusion of GNSS-RTK, INS and LiDAR for autonomous driving. 2020 IEEE/ION Position, Location and Navigation Symposium (PLANS). IEEE.

[12] Johannessen, E., Offermans, G., Bartlett, S., Grebnev, A., Bransby, M., & Williams, P., et al. (2014). Eloran initial operational capability – providing resilient pnt to mariners.
[13] Yang, X., Liu, W., Chen, F., Lu, Z., & Wang, F.. (2019). Analysis of the effects power-inversion (pi) adaptive algorithm have on gnss received pseudorange measurement. IEEE Access, PP(99), 1-1.
[14] Hong-Tuo, S., Chang-Qing, W., & Ji-Dong, F. . (2004). Current situation and development of anti-jamming technology of gps system in usa. Electro-optics & Passive Countermeasures.
[15] Jin, Y., Zhang, H. , Lu, T. , Yang, H. , & Gulliver, T. A. . (2020). A Two-Channel Constrained Power Inversion Algorithm for the Beidou Navigation Satellite System. 2019 IEEE Global Communications Conference (GLOBECOM). IEEE.
[16] Dai, X., Nie, J. , Chen, F. , & Ou, G. . (2017). Distortionless space-time adaptive processor based on mvdr beamformer for gnss receiver. Iet Radar Sonar & Navigation, 11(10), 1488-1494.
[17] Chang, C. L., & Huang, G. S..(2012). Spatial compressive array processing scheme against multiple narrowband interferences for gnss. 1-6.
[18] Wei, C. , Liu, J. , Zhang, F. , & Liu, P. . (2012). The comparison of two adaptive anti-jamming algorithm of navigation reciever. Proceedings of the 3rd China Satellite Navigation Academic Annual Conference-S07 Beidou/GNSS User Terminal Technology
[19] Chen, F. , Nie, J. , Ni, S. , Li, Z. , & Wang, F. . (2017). Combined algorithm for interference suppression and signal acquisition in gnss receivers. Electronics Letters, 53(4), 274-275.
[20] Qin, S. , Zhang, Y. D. , Amin, M. G. , & Himed, B. . (2017). DOA estimation exploiting a uniform linear array with multiple co-prime frequencies. Signal Processing, 130(1), 37-46.
[21] Ji, J., Zhang, J., Lu, H., Liu, Y., Wu, D., & Chen, W. (2020). A Single-Frequency Real-Time Lane-Level Positioning Method for Vehicle Safety. IEEE Access, 8, 185651-185664.

AN ADAPTIVE CUBATURE KALMAN FILTER ALGORITHM FOR PASSIVE LOCATION

PENG HAOJIE [1], ZHANG JIE[2], SHI WEISHENG[2]

[1] School of Aeronautics, Northwest Polytechnic University, Xi'an 710000, China
[2] Chengdu Aircraft Design& Research Institute, Chengdu 610000, China
E-MAIL: 10917636@qq.com

Abstract:

Modern stealth fighters usually keep the radar silent during the flight mission. In order to ensure the stealth performance, the integrated electronic warfare system generally uses the electronic support measures for passive detection. It locks the target's position by receiving radiation from the target sensor. In this paper, the aircraft flight maneuver model is established. The interactive multiple model is used to describe the motion state of aircraft. Residual and innovation is used improve cubature kalman filter to adaptive cubature kalman filter. Cubature kalman filter and adaptive cubature kalman filter were used for filtering respectively, and compared the effect. Then analyzed their root mean square error.

Keywords:

Electronic support measures; Interacting multiple model; Cubature kalman filter; Adaptive cubature kalman; Aircraft; Residual; Innovation; Root mean square error

1. Introduction

Passive detection technology is an important part in air combat. It is in the first O (observation) of OODA loop [1]. For modern stealth aircraft, it needs to keep its own radio frequency stealth before attack. The main environmental situation information comes from data link and its own passive detection system. Without intelligence support, passive detection is the only information source. In addition to avoiding interception, passive detection has the advantages of countering jamming and anti-radiation missile [2-3]. The development of passive detection technology is an important issue in the military field.

The rest of paper is organized as follows. Section 2 introduces the 3-DOF model used for aircraft model design. Section 3 details the cubature kalman filter (CKF) and then designs the adaptive cubature kalman filter (ACKF). Section 4 designs the interacting multiple model (IMM). Section 5 presents the corresponding simulation results and analyses of root mean square error (RMSE). At last, Section 6 concludes this paper.

2. Motion model

The target aircraft particle motion equation is established in the NED coordinate system to reflect the track of the aircraft. The 3-DOF model is sufficient to this paper. The 3-DOF model is established as formula (1-6).

Particle dynamics equation:

$$\dot{V} = g(n_x - \sin\theta) \tag{1}$$

$$\dot{\theta} = \frac{g(n_z \cos\gamma - \cos\theta)}{V} \tag{2}$$

$$\dot{\varphi} = \frac{g(n_z \sin\gamma)}{V\cos\theta} \tag{3}$$

V is flight speed;
θ is the velocity inclination Angle;
φ to course Angle;
nx is aircraft tangential overload;
nz is normal overload of aircraft;
γ is roll Angle;

Kinematics equation:

$$\dot{\mathrm{X}} = \mathrm{V}\cos\theta\cos\varphi \tag{4}$$

$$\dot{\mathrm{Y}} = \mathrm{V}\cos\theta\sin\varphi \tag{5}$$

$$\dot{\mathrm{Z}} = -\mathrm{V}\sin\theta \tag{6}$$

X, Y, Z are the position coordinates of the aircraft in the NED coordinate system.

3. Cubature Kalman filter

Cubature Kalman filter (CKF) is an excellent performance algorithm to solve the integration of higher-dimensional functions, which has linear complexity. It was proposed by Arasatnam and Haykin in 2009 [4]. The CKF algorithm uses the spherical radial integration criterion and the three order spherical diameter. Then through the cubature rule to solve the problem [5].

For nonlinear discrete-time systems as formula (7-8):

$$x_t = f(x_{t-1}) + v_{t-1} \tag{7}$$

$$y_t = h(x_t) + \omega_t \tag{8}$$

The process noise and measurement noise are independent of each other and have the following statistical characteristics:

$$v_{t-1}\sim \mathrm{N}(0, Q_{t-1})$$
$$\omega_t\sim \mathrm{N}(0, R_t)$$

CKF needs to calculate cubature points and use the weighted sum of 2n cubature to approximate the Gauss-Hermit integral. In order to solve the arbitrary distribution function and integral problem by the cubature integral criterion, it can be expressed as formula (9):

$$\int_{R^{n_x}} f(x)\mathrm{N}(x;0,I_{n_x})dx \approx \left(\sum_{i=1}^{m}\omega_i f\left(\mu+\sqrt{P}\xi_i\right)\right)/\mathrm{I}$$
$$\mathrm{m}=2n_x$$
$$\xi_i=\sqrt{m/2}[I]_i \quad (9)$$
$$\omega_i=\frac{1}{m},(i=1,2,\dots,m)$$
$$[I]\epsilon R^{n_x}$$
$$[I]_i\in\left\{\begin{pmatrix}1\\0\\\cdot\\\cdot\\\cdot\\0\end{pmatrix},\begin{pmatrix}0\\1\\\cdot\\\cdot\\\cdot\\0\end{pmatrix},\dots,\begin{pmatrix}0\\0\\\cdot\\\cdot\\\cdot\\1\end{pmatrix},\begin{pmatrix}-1\\0\\\cdot\\\cdot\\\cdot\\0\end{pmatrix},\begin{pmatrix}0\\-1\\\cdot\\\cdot\\\cdot\\0\end{pmatrix},\dots,\begin{pmatrix}0\\0\\\cdot\\\cdot\\\cdot\\-1\end{pmatrix}\right\}$$

The mean of the normal distribution is μ, the covariance is P, ω_i is the weight of the cubature point, ξ_i is the set of diffusion cubature points, and "I" is the equal weight of cubature points.

The operation steps of CKF include prediction and filtering.

Initialization: Set the initial value $x_0\sim\mathrm{N}(\hat{x}_{0|0},P_{0|0})$; calculate and store the weighted sigma point $\{\xi_i,\omega_i\}$.

Prediction: Calculate the t-1 state posterior probability density $\mathrm{N}(\hat{x}_{t-1|t-1},P_{t-1|t-1})$, which corresponding the sigma point as formula (10-11):

$$P_{t-1|t-1}=S_{t-1|t-1}S_{t-1|t-1}^T \quad (10)$$
$$\xi_{i,t-1}=S_{t-1|t-1}\xi_i+\hat{x}_{t-1|t-1} \quad (11)$$

Predicted probability density function of the state$\mathrm{N}(\hat{x}_{t|t-1},P_{t|t-1})$ can be calculate as formula (12-14):

$$\chi_{i,t-1}=f\left(\xi_{i,t-1}\right) \quad (12)$$
$$\hat{x}_{t|t-1}=\sum_{i=1}^{m}\omega_i\chi_{i,t|t-1} \quad (13)$$
$$P_{t|t-1}=\left(\sum_{i=1}^{m}\omega_i(\chi_{i,t-1}-\hat{x}_{t|t-1})(\chi_{i,t-1}-\hat{x}_{t|t-1})^T\right)+Q_{t-1} \quad (14)$$

Filtering: calculate the sigma points corresponding to the predicted probability density function of the state $\mathrm{N}(\hat{x}_{t-1|t-1},P_{t-1|t-1})$ as formula (15-16):

$$P_{t|t-1}=S_{t|t-1}S_{t|t-1}^T \quad (15)$$
$$\pi_{i,t}=S_{t|t-1}\xi_i+\hat{x}_{t|t-1} \quad (16)$$

The variance of innovation, prediction and state measures calculated as formula (17-20):

$$\psi_{i,t}=h(\pi_{i,t}) \quad (17)$$
$$\hat{y}_t=\sum_{i=1}^{m}\omega_i\psi_{i,t} \quad (18)$$
$$P_{yy}=\sum_{i=1}^{m}\omega_i(\psi_{i,t}-\hat{y}_t)(\psi_{i,t}-\hat{y}_t)^T+R_t \quad (19)$$
$$P_{xy}=\sum_{i=1}^{m}\omega_i(\chi_{i,t}-\hat{x}_{t|t-1})(\psi_{i,t}-\hat{y}_t)^T \quad (20)$$

The filtering probability density of the state at time t calculate as formula (21-23):

$$K_t=P_{xy}P_{yy}^{-1} \quad (21)$$
$$\hat{x}_{t|t}=\hat{x}_{t|t-1}+K_t(y_t-\hat{y}_t) \quad (22)$$
$$P_{t|t}=P_{t|t-1}-K_tP_{yy}K_t^T \quad (23)$$

3.1. Adaptive improvement strategy

In the real environment, the situation is very complex. It is difficult to measure measurement noise accurately, because noise is constantly changing. Therefore, in order to make the measurement error covariance matrix can be automatically adjusted. Adaptive improvement based on innovation and residual sequence [6-7].

Innovation sequence can be calculated as formula (24):

$$\delta_t=y_{t+1}-h(\hat{x}_{t|t-1}) \quad (24)$$

Based on the sample data, the covariance matrix of the innovation is approximately estimated as formula (25):

$$E(\delta_t\delta_t^T)=\frac{1}{N}\sum_{i=1}^{N-1}\delta_{t-i}\delta_{t-i}^T=P_{yy} \quad (25)$$

Residual sequence can be calculated as formula (26):

$$\eta_t=y_{t+1}-h(\hat{x}_{t|t}) \quad (26)$$

The estimated value of the measurement noise covariance matrix be updated as formula (27):

$$R_t=\frac{1}{N}\sum_{i=1}^{N-1}\delta_{t-i}\delta_{t-i}^T-\sum_{i=1}^{m}\omega_i\psi_{i,t-i}(\psi_{i,t-i})^T-\hat{y}_{t-i}(\hat{y}_{t-i})^T \quad (27)$$

Based on the sample data, the covariance matrix of residuals is approximately estimated as formula (28):

$$E(\eta_t\eta_t^T)=\frac{1}{N}\sum_{i=1}^{N-1}\eta_{t-i}\eta_{t-i}^T \quad (28)$$

Updated the estimated value of the process noise covariance matrix as formula (29):

$$Q_t=\frac{\left(t*Q_{t-1}+\frac{1}{N}\sum_{i=1}^{N-1}\eta_{t-i}\eta_{t-i}^T+h*P_{t|t}h^T\right)}{t+1} \quad (29)$$

4. IMM model

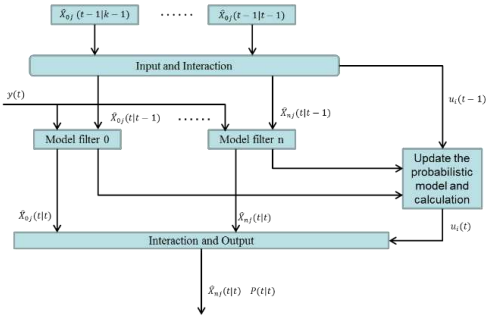


Fig.1 IMM flow

IMM is a soft switching algorithm proposed by H.Blom in 1984 [8]. It is widely used in the field of maneuvering target tracking and overcomes the problem of large model estimation error by perform system transformation estimation through effective weighted fusion, as in Figure 1[9].

Input interaction (step 1)

The prediction probability (normalization constant) of the model as formula (30):

$$\bar{c}_j = \sum_{i=1}^{r} P_{ij}\mu_{ij}(t-1) \quad (30)$$

The probability of mixing between model transfers as formula (31):

$$\mu_{ij}(t-1|t-1) = \sum_{i=1}^{r} P_{ij}\mu_{ij}(t-1)/\bar{c}_j \quad (31)$$

Estimation of mixed state model as formula (32):

$$\hat{X}_{0j}(t-1|t-1) = \sum_{i}^{r} \hat{X}_i(t-1|t-1)\mu_{ij}(t-1|t-1) \quad (32)$$

The mixed covariance is estimated as formula (33):

$$P_{0j}(t-1|t-1) = \sum_{i}^{r} \mu_{ij}(t-1|t-1)\{P_i(t-1|t-1) + \left[\hat{X}_i(t-1|t-1) - \hat{X}_{0j}(t-1|t-1)\right]\left[\hat{X}_i(t-1|t-1) - \hat{X}_{0j}(t-1|t-1)\right]\left[\hat{X}_i(t-1|t-1) - \hat{X}_{0j}(t-1|t-1)\right]^T\} \quad (33)$$

ACKF filtering (step 2)

$\hat{x}_{0j}(t-1|t-1)$, $P_{0j}(t-1|t-1)$, y(t) as input, and as formula (11~29).

Model probability update (step 3)

The likelihood function is used to update the model probability $\mu_j(t)$. The likelihood function is as formula (34):

$$\Lambda_j(t) = \frac{1}{(2\pi)^{n/2}|S_j(t)|^{1/2}} \exp\left\{-\frac{1}{2} v_j^T S_j^{-1}(t) v_j\right\} \quad (34)$$

$$v_j(t) = y(t) - h(t)\hat{X}_j(t|t-1)$$

$$S_j(t) = h(t)P_j(t|t-1)h(t)^T + R(t)$$

The probability of model j is as formula (35):

$$\mu_j(t) = \Lambda_j(t)\bar{c}_j/c \quad (35)$$

c is the normalized constant, $c = \sum_{j=1}^{r} \Lambda_j(t)\,\bar{c}_j$

Output the interaction (step 4)

Based on the model probability, the total state estimation and the total covariance estimation as formula (36-37):

$$\hat{X}(t|t) = \sum_{j=1}^{r} \hat{X}_j(t|t)\mu_j(t) \quad (36)$$

$$\hat{P}(t|t) = \sum_{j=1}^{r} \mu_j(t)\left\{P_j(k|k) + \left[\hat{X}_j(t|t) - \hat{X}(t|t)\right].\left[\hat{X}_j(t|t) - \hat{X}(t|t)\right]^T\right\} \quad (37)$$

5. Simulation experiment design and result analysis

By using the common flight simulation software with the aircraft model, the target aircraft flies through several navigation points and the tested aircraft park at the airport as the origin. The tested aircraft is mounted with two ESM module of electronic warfare with CKF-IMM and ACKF-IMM filter respectively. The aircraft patrols in the mission area with uniform motion, uniform acceleration and turning. The initial condition height is set to 9000 m and $X_t = [x\ \dot{x}\ \ddot{x}, y\ \dot{y}\ \ddot{y}]^T$ is the target aircraft state including the position, velocity and acceleration in the X and Y axis. It outputs the aircraft data of each simulation step. This paper needs to observation altitude, latitude and longitude. It convert latitude, longitude and altitude into the distance and bearing from the observation point with the random noise. The simulation is set to 200 second, and sample every 1 second. First, the target aircraft flies at a constant speed of $\dot{x} = 300\text{m/s}$ along the X axis from west to east. After 10 seconds it accelerates to 350m/s with $\ddot{x} = 5\text{m/s}$ acceleration. After 40s it turns southward at 350m/s. Then aircraft flies westward along X acceleration -5m/s, and flies at 300m/s for 10s, turns northward. After 20 seconds, it returns to the original position, as in Figure 2[10].

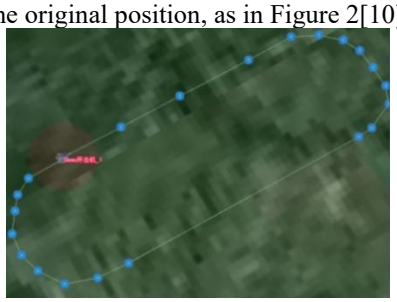


Fig.2 Aircraft track simulation

Define the mean value of filtering error:

$$\overline{e_x(t)} = \frac{1}{M}\sum_{i=1}^{M}[x_i(t) - \hat{x}_i(t|t)] \quad (38)$$

Define the root-mean-square error of filtering:

$$\sigma_{\hat{x}} = \sqrt{\frac{1}{M}\sum_{i=1}^{M}[x_i(t) - \hat{x}_i(t|t)]^2 - \left[\overline{e_x(t)}\right]^2} \quad (39)$$

M is the number of Monte Caerlo simulation.

As formula (38~39), through the simulation test, it can

be found that the filtering effect of ACKF-IMM is much better than that of CKF-IMM in the period of rapid speed change, except that RMSE is slightly worse than CKF-IMM in 20-50 seconds. In the whole simulation process, the error fluctuation of ACKF-IMM is relatively gentle, which proves that it can adapt to the speed change better, as in Figure 3.

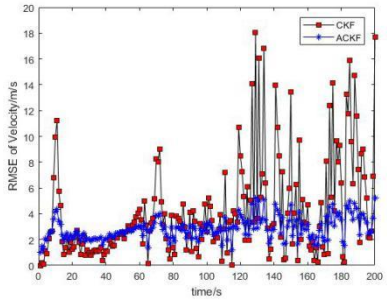


Fig.3 RMSE of Velocity

By analyzing and comparing the RMSE of range, it can be found that the error of CKF-IMM mostly fluctuates between 1500 meters and 500 meters, while ACKF-IMM effectively suppresses the error within 500 meters. In nonlinear motion, CKF-IMM will have large error, and the error mainly occurs in aircraft turning maneuver period. Through comparison, although the RMSE of ACKF-IMM fluctuates in the turning maneuver phase, it is far less than that CKF-IMM is so fierce. This proves that ACKF-IMM has good stability, as in Figure 4.

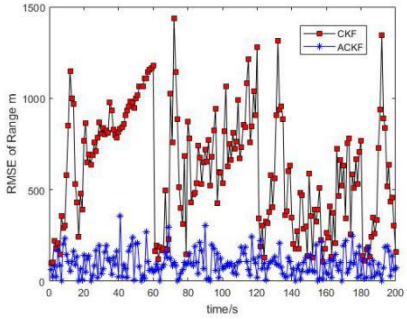


Fig.4 RMSE of Range

6. Conclusions

In this paper, the traditional CKF is improved to ACKF which is used as filter of IMM algorithm. The adaptive ability reduces the error especially on the range error and makes the error fluctuation relatively gentle, thus improving the precision of the filtering algorithm. Simulation results show that ACKF algorithm has good adaptability and stability in target maneuver filtering.

References

[1] Yun P, Tiedan H, Qingshan Y, et al, "Analysis of Fighter Agility in Beyond-visual-range Air Combat", Air & Space Defense, No. 1, pp. 42-46, Jan. 2019.

[2] Yang Lin, Zhou Yiyu and Sun Zhongkang, "PASSIVE LOCATION AND ACCURACY ANALYSIS USING TDOA INFORMATION OF MULTI-STATIONS", CHINESE JOURNAL OF AERONAUTICS, Vol 11, No. 1, pp. 37-43, Jan. 1998.

[3] Zachary Lum. KillinEW on the offensive",Journal of electronics defense, Vol 20, No. 7, pp. 37-39, Jul.1997

[4] K. Salahshoor, M. Mosallaei and M. Bayat, "Centralized and decentralized process and sensor fault monitoring using data fusion based on adaptive extended Kalman filter algorithm", Measurement, Vol 41, No. 10, pp. 1059-1076, Jun. 2008.

[5] I. Arasaratnam and S. Haykin, "Cubature Kalman Filters", IEEE Transactions on Automatic Control, Vol 54, No. 6, pp. 1254-1269, July. 2009.

[6] Hongwei Wang, Wei Zhang, Junyi Zuo and Heping Wang, "Generalized cubature quadrature Kalman filters: derivations and extensions", Journal of Systems Engineering and Electronics, Vol 28, No. 3, pp. 556-562 , Jun. 2017.

[7] Z. B. Yang, F. C. Guo and Y. Y. Zhou, "Iterated IMM algorithm for maneuvering target tracking by a single passive observer", Journal of Astronautics, Vol 29, No. 1, pp. 304-310, Jan. 2008.

[8] Blom. H. A. P and Y. Bar-Shalom. "The interacting multiple model algorithm for systems with Markovian switching coefficients", IEEE Transactions on Automatic Control, Vol 33, No. 8, pp. 780-783, Aug. 1988.

[9] Gao Liang and et al, "Improved IMM Algorithm for Nonlinear Maneuvering Target Tracking", Procedia Engineering, Vol 29, pp. 4117-4123, Dec. 2012.

[10] Yuan. G, Zhu. W, Wang. W,and Yin. B "Maneuvering Target Tracking Algorithm Based on Interacting Multiple Models", Mathematical Problems in Engineering, pp. 1-7, Mar. 2015.

EXPLORATION OF DIFFUSION LMS OVER STATIC AND ADAPTIVE COMBINATION POLICY

CHIKWENDU A. IJEOMA[1], MD A HOSSIN[2], HAILEGIORGIS A BEMNET[3], ALULA A. TESFAYE[4], AMARE H. HAILU[5], CHIKWENDU N. CHIAMAKA[6]

[1,3]School of Information and Communication Engineering, University of Electronic Science and Technology of China
[2] School of Management Science, University of Electronic Science and Technology of China
[4]School of Mechanical and Electrical Engineering, University of Electronic Science and Technology of China
[5]School of Computer Science, University of Electronic Science and Technology of China
[6]Department of Accounting, Faculty of Management Sciences, University of Port Harcourt, River State, Nigeria
E-MAIL: amauchefelix@gmail.com, altabbd@uestc.edu.cn, bemnian.amsalu@gmail.com, abeltesfaye073@gmail.com, haymih34@gmail.com, amakafelix21@gmail.com

Abstract:

In recent years, Diffusion LMS algorithm has been thoroughly researched. This powerful approach enables distributed problem optimization over sensor networks to be solved. The best parameter vectors for all agents is likely not to be the same in such implementations. In addition, agents typically share information through noisy links. Here, we compared the average performance of some major distributed network-based combination policies: Static Combination Policy (metropolis policy and relative variance combination policy) and adaptive Combination Policy. The diffusion of information gathered from neighbors is an important problem in creating adaptive networks in as much as the network mean-square performance is dependent on the preference for combined weights. The aspect of the best selection of the combination weights is considered. We showed the adaptive combination policy outperformed the two analyzed static combination policy over noisy links. Also note that because we considered linearly complex algorithms in a single-task LMS diffusion, we analyzed the theoretical performance within a collaborative target tracking problem.

Keywords:

Diffusion strategy; Adaptive networks; Mean-square stability; Combination weights; Mean square-error performance

1. Introduction

Distributed optimization enables deferential problems to be solved decentrally across networks, where nodes may share information amongst neighbors to boost local estimates. Each node is concerned with estimating the same vector parameter in single-task networks. Our interest is in the diffusion strategies [1-4] as they are efficient, robust and allow continuous learning, as part of the current rules for cooperation on single-task issues. Diffusion LMS is an effective solution technique for co-operating agents to solve distributed optimization problems. To date, multiple algorithms with distributed estimates were proposed including the, diffusion Recursive Least Square (dRLS) [5], diffusion Least Mean Square (dLMS) and diffusion Total-Least-Square (dTLS) [6]. The LMS Algorithm has been more thoroughly explored in a number of situations because of the inherently basic process [7].

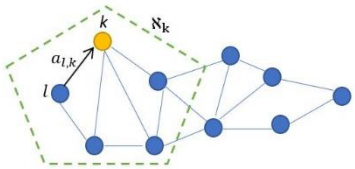


Fig.1 Diffusion Network schematic illustration showing agent k neighborhood

Diffusion LMS is a single purpose algorithm. However, it can be predicted that diffusion LMS can be used in such multi-task settings due to faulty simulation hypothesis or a willful lack of small task variations. Diffusion techniques are applied in two stages: adaptation and combination. Every node gathers information from its neighbors in the combination stage. Each of the network's nodes updates their own estimates by LMS algorithms during adaptation. Two diffusion algorithms called ATC (Adapt-then-Combine) and the CTA (Combine-then-Adapt) diffusion LMS algorithms are mentioned in the implementation order of the two phases in [4]. The nodes share their knowledge with the nearby neighbors in both diffusion LMS algorithm and fuse the estimates obtained by linear combinations. In the efficiency

of the adaptive networks, the combination weights of every neighbor are very important and play a significant role [8].

We examined both the static (Metropolis rule [9]) and adaptive combination policies applying different metrics in order for the nodes noise level to be analyzed and for a significant convergence rate to be achieved as well as steady state error. The analysis also confirms that diffusion strategies allow information for more thorough dissemination via networks under constant step-size and this property has a positive impact on network evolution. Diffusion networks converge faster and achieve lower mean-square deviation and are indifferent to the preference of combination weights in their mean-square stability. We have also shown that individual node stability is adequate to guarantee the diffusion network stability irrespective of the combination weight. The study also indicates that diffusion techniques provide an efficient means of improving networks' coordination. They act in order to still preserve secure diffusion networks, independent of combination topology.

2. Diffusion LMS Estimation Strategies Over Networks

Take for instance a network of linked nodes *N*, each *k* of collected data has access to sequences of temporary measurement$\{d_k(j), x_i(j)\}$. $d_k(j)$ refers to the zero-mean scalar measurement (reference signal), $x_k(j)$ refers to a zero mean $L\,x\,1$ regression vector with a +ve covariance matrix $R_{x,k} = Ex_k(j)x_k^T(j)$. The data gotten at node k is designed to be dominated by the linear model.

$$d_k(j) = x_k^T(j)w_k^* + z_k(j) \quad (1)$$

Where w_k^* are *(L x 1)* weight vectors at node k which are unknown and $z_k(j)$ refers to a zero-mean measurement noise at node k at an absolute time n. The noise has variance $\sigma_{z,k}^2$ and is distinct from every other signal. To calculate the unknown $(L\,X\,1)$ Weight vectors at node k indicated by w_k^* , let the mean-square-error cost function related to node k be noted as $J_k(w)$, the global cost function for the network can be summarized below as;

$$J^{glob}(w) = \sum_{k=1}^{N} J_k(w) \quad (2)$$

Where

$$J_k(w) = E\{|d_k(j) - x_k^T(j)w|^2\} \quad (3)$$

Looking at a single Task environment, where a linked network $G = (v, \varepsilon)$ defined by a set $v = \{1, 2, \ldots N\}$ of *N* agents, alongside a set ε of edges that are 2-element subsets of v, We suppose all nodes calculate the same vector parameter $w_k^* = w^*$ for all k. LMS diffusion strategy collaboration among nodes enhances network output estimation accuracy. However, given a multitasking setting, the true weight vectors on various nodes will vary from each other. i.e. $w_k^* \neq w^*$ thus, cost function $J_k(w)$ may not have the same optimum vector w_k^*.

3. Diffusion Strategy Implementation

3.1. Non-Interactive Strategy

As its name means, every *Node* interacts with the other nodes independently. The operation of a local LMS adaptive filter is applied to w^* data $\{d_k(j), u_{k,j}\}$. Pointing to [10-11], The filter update is presented as;

$$w_{k,j} = w_{k,j-1} + \mu_k u_{k,j}^*[d_k(j) - u_{k,j}w_{k,j-1}] \quad (4)$$

Where $\mu_k > 0$ = the step-size which is constant and used by node k. [4] Explain the vector more, $w_{k,j}$ refers to the estimate for w^0 which at time j, is being computed by node k. it is worth also to agree that models where $R_{u,k} > 0$ for all k, we can apply reference [12] in all the individual nodes to estimate w^0.

3.2. Interactive Strategy

Nodes communicate and collaborate with neighbors in the interactive strategy mode of operation by exchanging information. The collaborative approach researchers have used is wide: Consensus strategy, Adapt-Then- Combine (ATC) diffusion strategy, Combine-Then-Adapt (CTA) diffusion strategy. The ATC diffusion LMS [13-14] was taken into consideration in this article.

$$\psi_k(j+1) = w_k(j) + \mu_k \sum_{l \in N_k} c_{lk}x_l(j)[d_l(j) - x_l^T(\mathrm{j})w_k(j)]$$
$$w_k(j+1) = \sum_{l \in N_k} a_{lk}\psi_l(j+1) \quad (5)$$

Where ψ_k = a +ve step-size parameter at k node while (6) $w_k(j)$ = the estimate of w^* at k node and iteration j. c_{lk} and a_{lk} are the non-negative co-efficient used to scale the data $\{x_l(j)[d_l(j)\}$. If node *l* is not linked to node k, i.e, $l \notin N_k$,the intermediate estimate $\psi_l(j+1)$ transferred from node *l* to node *k* are zero.

ATC algorithm (5)(6) transmits information at every step from node $l \in N_k$ to node k in the presence of noisy communication links thus transforming the ATC Diffusion LMS algorithm to be;

$$\psi_k(j+1) = w_k(j) + \mu_k \sum_{l \in N_k} c_{lk}x_l(j)[d_l(j) - x_l^T(\mathrm{j})w_k(j)] \quad (7)$$

4. Performance Analysis

We analyzed under the static combination rule, the performance of the relative variance policy and the metropolis policy in noisy link. The relative variance achieves lower steady state mean square error and converges faster. Due to space limitation, we will refer to [16] for the analysis of MSD (Mean Square Deviation) of the network.

$$MSD \triangleq \lim_{i\to\infty} \frac{1}{N} \sum_{k=1}^{N} \mathbb{E} \left\| \widetilde{W}_{k,i} \right\|^2 \quad (8)$$

When we have small step size and all the nodes regression vector is spatially and temporarily not dependent, the adaptive network's MSD can be entered as follows;

$$MSD \approx \frac{1}{N} vec\,(\mathbb{Y}^{\boldsymbol{T}})^{\boldsymbol{T}} (\boldsymbol{I}-\boldsymbol{F})^{-\mathbf{1}} vec(\boldsymbol{I}) = \frac{1}{N} \sum_{j=0}^{\infty} Tr\left[\boldsymbol{X}^{j} \boldsymbol{Y} (\boldsymbol{X}^{*})^{j}\right] \quad (9)$$

Where F, X, Y, R and G demotions can be seen in reference [16]. On Assumptions that $\mu_k = \mu$ for all k i.e. indistinguishable step sizes among all the nodes and covariance matrix $\{\boldsymbol{R}_{u,k}\}$ of regressors $\{\boldsymbol{U}_{k,i}\}$ is not changed towards the network, the MSD equation is rewritten as;

$$MSD \approx \frac{\mu^2}{N} \sum_{j=0}^{\infty} Tr\left[\boldsymbol{R}_u (\boldsymbol{I}-\boldsymbol{\mu R}_u)^{\mathbf{2}j}\right] \boldsymbol{Tr}\left[(\boldsymbol{A}^{T})^{J+1} \boldsymbol{V} \boldsymbol{A}^{\boldsymbol{j+1}}\right] \quad (10)$$

take $\mathbf{V} = \mathbf{diag}\ \{\sigma_{v,1}^2, \ldots \sigma_{v,N}^2\}$

$$C_{l,k} = \begin{cases} 1/\max(n_{l,k}, n_{k),}\ if\ l\ \varepsilon\ N_k, l \neq k \\ 1 - \sum_{l\neq k} c_{l,k}, if\ l = k \\ 0, otherwise. \end{cases} \quad (11)$$

For the rule of Metropolis (11) and the rule of relative variance (12), we use the above rule for the achievement of the MSD having a basis on the static combination rule is stated as

$$C_{l,k} = \begin{cases} \frac{\sigma_{v,l}^{-2}}{\sum_{m\in N_k} \sigma_{v,m}^{-2}}, if\ k \neq l\ are\ neighbours\ or\ k = l \\ 0, \quad otherwise \end{cases} \quad (12)$$

Where $\sigma_{v,l}^{-2}(i) = (1 - v_k)\sigma_{v,l}^{-2}(i-1) + v_k ||\Psi_{l,i} - W_{l,i-1}||^2$

We explored a comparatively instantaneous-error combination policy as illustrated in [16] while evaluating the adaptive combination rule against the static combination rule.

$$C_{l,k} = \begin{cases} \frac{|e_1|^{-1}}{\sum_{m\in N_k} |e_m|^{-1}}, for\ l \in N_k \\ 0, \ otherwise \end{cases} \quad (13)$$

Where diffusion networks are considered by assigning greater proportions to lower noise power nodes. In Equation 5, when we have a small step size around the network and the ATC diffusion LMS algorithm reaches a stable situation, the intermediate estimate $\Psi_{k,i}$ reaches w^*.

5. Simulation Results

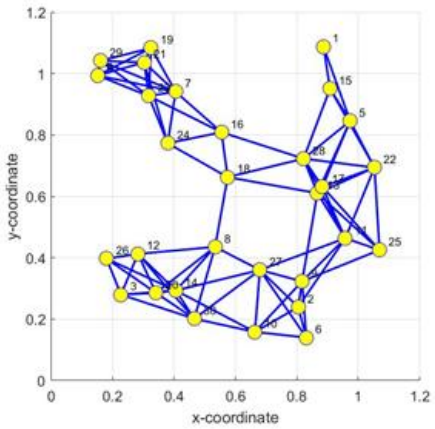


Fig.2 Network Topology

Here, we simulate the performance of the mean-square comparing static and the adaptive combination rule over noisy links within a collaborative target tracking problem. The metropolis rule (11) relative variance (12) and RIE combination policy (13) have been compared. In our simulation, each nodes level noise is randomly generated. Throughout all agents, we set uniformly $\boldsymbol{\mu}_k = 0.05$ (step sizes) and noise variances are randomly generated over [-25, -15] dB and all $R_{u,k}$ are the same in all aspect. The network topology here consists of 30 Nodes and is structured to identify nodes as neighbors if the gap between different nodes is equal or below to a lower limit value which is shown in Fig. 2. The boundary of two nodes demonstrates their neighborhood. Fig.3 displays the outcomes of the simulation. We see that the concept of the metropolis rule is outperformed by the relative variance combination rule. As is obvious, it is not best to settle on combination weights, as presented by the metropolis, since the weights do not consider the noise profile in the node. We observe in fig 3 that the adaptive rule achieves a seemingly lower MSD as compared to the other rules.

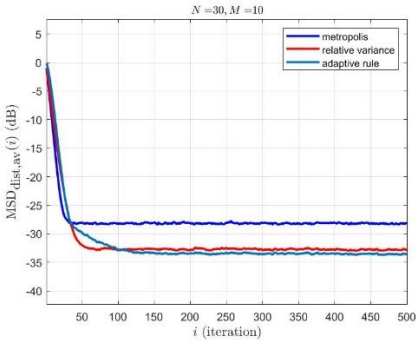


Fig.3 Average performance of all nodes

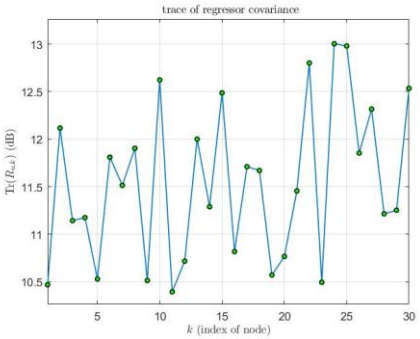


Fig.4 Trace of regressor covariance

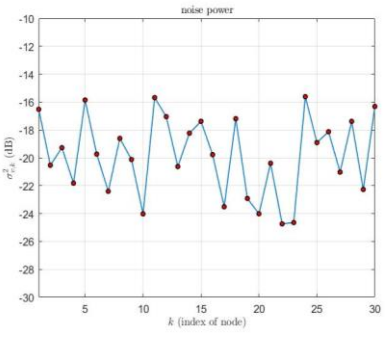


Fig.5 Noise Power across each Node under different combination policies

6. Conclusions

We compared analytically static combination polices and adaptive policies in ATC diffusion, for distributed estimation over noisy networks in a single Task. The results show that adaptive rule perform better than static. Besides that, the consistency of diffusion network is not dependent on the combination weights. our result simulation also proves that the adaptive combination strategy beats the current combination laws in respect to steady-state error.

References

[1] Lopes CG, Sayed AH. Diffusion least-mean squares over adaptive networks: Formulation and performance analysis. IEEE Transactions on Signal Processing. 2008 Jun 17;56(7):3122-36.

[2] Cattivelli FS, Sayed AH. Diffusion LMS strategies for distributed estimation. IEEE transactions on signal processing. 2009 Oct 6;58(3):1035-48.

[3] Chen J, Richard C, Sayed AH. Multitask diffusion adaptation over networks. IEEE Transactions on Signal Processing. 2014 Jun 27;62(16):4129-44.

[4] A. H. Sayed, "Adaptive networks," Proc. IEEE, vol. 102, no. 4, pp. 460–497, April 2014.

[5] Cattivelli FS, Lopes CG, Sayed AH. Diffusion recursive least-squares for distributed estimation over adaptive networks. IEEE Transactions on Signal Processing. 2008 Apr 15;56(5):1865-77.

[6] López-Valcarce R, Pereira SS, Pages-Zamora A. Distributed total least squares estimation over networks. In2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2014 May 4 (pp. 7580-7584). IEEE.

[7] Feuer A, Weinstein E. Convergence analysis of LMS filters with uncorrelated Gaussian data. IEEE Transactions on Acoustics, Speech, and Signal Processing. 1985 Feb;33(1):222-30.

[8] Zhao X, Sayed AH. Performance limits for distributed estimation over LMS adaptive networks. IEEE Transactions on Signal Processing. 2012 Jun 15;60(10):5107-24.

[9] Xiao L, Boyd S. Fast linear iterations for distributed averaging. Systems & Control Letters. 2004 Sep 1;53(1):65-78.

[10] Chen J, Sayed AH. Diffusion adaptation strategies for distributed optimization and learning over networks. IEEE Transactions on Signal Processing. 2012 May 9;60(8):4289-305.

[11] Towfic ZJ, Chen J, Sayed AH. On the generalization ability of distributed online learners. In2012 IEEE International Workshop on Machine Learning for Signal Processing 2012 Sep 23 (pp. 1-6). IEEE.

[12] Tu SY, Sayed AH. Mobile adaptive networks. IEEE Journal of Selected Topics in Signal Processing. 2011 Mar 10;5(4):649-64.

[13] Tu SY, Sayed AH. Diffusion strategies outperform consensus strategies for distributed estimation over adaptive networks. IEEE Transactions on Signal Processing. 2012 Sep 6;60(12):6217-34.

[14] Lopes CG, Sayed AH. Diffusion least-mean squares over adaptive networks: Formulation and performance analysis. IEEE Transactions on Signal Processing. 2008 Jun 17;56(7):3122-36.

[15] Tu SY, Sayed AH. Optimal combination rules for adaptation and learning over networks. In2011 4th IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP) 2011 Dec 13 (pp. 317-320). IEEE.

[16] Wang J, Dai F, Yang J, Gui G. Efficient combination policies for diffusion adaptive networks. Peer-to-Peer Networking and Applications. 2020 Jan 1;13(1):123-36.

AUTOMATIC ROOM TEMPERATURE CONTROL SYSTEM USING ARDUINO UNO R3 AND DHT11 SENSOR

GURMU M. DEBELE[1], XIAO QIAN[2]

[1]Student, [2]Lecturer, School of Mechanical and Electrical Engineering, University of Electronic Science and Technology of China, Chengdu 611731
E-MAIL: mersimoidebele2027@gmail.com, 25133485@qq.com

Abstract:

This paper presents designing and implementing an Automatic room temperature control system using the Arduino and DHT11 sensor. The fan speed control system has also been proposed. Here, the user sets the minimum and the maximum reference temperature range from the keypad. The DHT11 sensor senses the surrounding room temperature and gives the result in degrees Celsius. Both the reference and the measured values are displayed on the Liquid Crystal Display (LCD). The Arduino microcontroller, being the processing unit of the system, gets the sensor's measured value and compares it with the set threshold. The results are: when the measured room temperature is less than the minimum of the threshold value; then, the microcontroller turns on the heater. If the measured room temperature is greater than the maximum threshold value, then the fan triggered on. The speed of the fan will be controlled by the pulse width modulation (PWM) technique based upon the temperature difference between the sensor reading and the maximum threshold. The larger the temperature difference, the larger the fan's duty cycles, and the faster its speed. Finally, if the room's measured temperature is between the setpoint range, all the loads are turned off. That means the room temperature is maintained normal.

Keywords:

Arduino Uno; DHT11(temperature and humidity) sensor; Keypad; Microcontroller; LCD (Liquid Crystal Display); Pulse width modulation (PWM).

1. Introduction

With the gradual advancement of technology, automation has become part of human life. In this regard, modern technologies have brought several innovations that automatically implement a particular task. Among these discoveries, microcontroller plays a vital role in the smart system of the electronic world. A microcontroller is a control system on a single chip that makes possible for the automation of the designed system and control process and produces precise results [1,2]. Among all places occupied by a human being, a home is the most important and needs to be maintained in the proper temperature. Nowadays, keeping living and working places at a conducive temperature is not only crucial to be healthy and productive, but also maintaining the room at average temperature helps to prevent spoiling of foods, medicine, and other goods in the room. Commonly, people use the manually controlled system, air-condition (AC), to regulate the temperature in their living environment. However, this manually operated system has notable limitations. The drawback is that if the user forgets to switch on or adjust the AC when the temperature becomes abnormal, children, disabled persons, and perishable items could be affected. The other problem with the mechanical AC system is, sometimes even if the air condition (AC) is still working, it is difficult to maintain the room temperature. Furthermore, if not appropriately managed, it may result in unnecessary expense and power usage. In general, its operations always require the user to turn it on and off regardless of the room temperature condition. Therefore, to address these drawbacks, the Automatic Room Temperature Control System is proposed. An automatic room temperature control system is a self-automated temperature control system [3] that can control the speed of the fan depending on the current room temperature. It comprised of a control unit (MCU), temperature sensor (DHT11), heater, fan, and keypad (3x4) to monitor the room temperature. According to the value of the ambient temperature, the microcontroller compares sensor temperature reading with a set value. Then the microcontroller makes a decision in accordance. This system's main advantages are easy to use, less energy usage, economical, more convenient to control temperature, and user-friendly.

2. Proposed system

The proposed system is an automatic self-regulating system that use the fan speed control system, the heater and the keypad to automatically monitor the room temperature

depending on the current room temperature and the predefined reference temperatures. Arduino is used for the central controlling system. The keypad is used to input the reference temperature ranges. Every time the users need to change (set) his /her own desired range of temperature, they use the keypad device to set the ranges of temperature values. In this case, the user can set his / her own desired reference temperature anytime. The sensor senses the temperature and sends it to the Arduino microcontroller. Afterwards, the microcontroller compares the sensor read value with the setpoint, then automatically makes a decision. If the temperature is below the minimum of the reference room temperature, then the heater automatically turned on to warm up the room until the temperature gets back to the desired value and then turned off [4]. If the room temperature is larger than the maximum of the desired room temperature, then the microcontroller automatically triggered on the fan to cool the room until it returns to the desired value and then turned off [4]. The fan's speed is controlled and changed based upon the current temperature and the maximum of the reference temperature [5]. Fig.1 demonstrates the block diagram of the proposed automatic room temperature control system. The Arduino Uno being the heart of this system, accessed the inputs signal from the DHT11 sensor's serial data (output) pin. The analogue-digital converter (ADC) converts the accessed information into an equivalent digital value and execute them one by one. Additionally, the microcontroller allows the relay switch to control and monitor the heater and fan's operation.

In this project, we proposed the fan speed control system [1,2,4,5,6,8] as well. Pulse width modulation techniques (PWM) is introduced to control the speed of the fan. In this case, the pulse width modulation (PWM) will significantly control the power supplied to the fan. The status of the speed of the fan is divided into zero speed, slow speed, medium speed, fast speed, and very-fast speed [6]. The relay switches keep both the fan and the heaters from damage due to overcurrent. Both the fan and the heater used an external power supply of 12V battery while Arduino used a maximum input voltage of 5V.

The signal from the microcontroller passed through a network of transistors (BC108 NPN bipolar junction transistor). The base is connected to a resistor. Both the collector and the emitter are connected to diode, relay switch and ground in series. Fig.1 below shows the block diagram of the proposed system of this project.

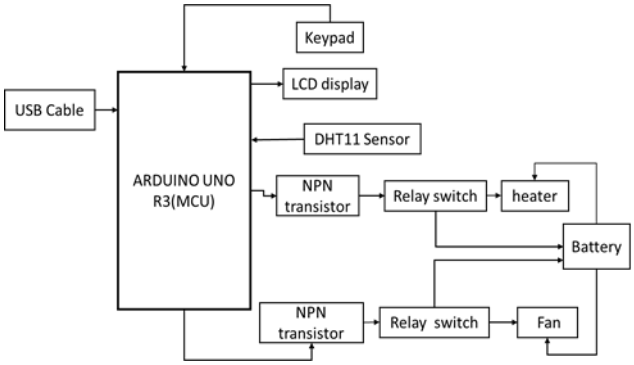


Fig.1 Block diagram of the proposed system

The microcontroller measures the temperature from the Digital Integrated Circuit (DIC) DHT11 sensor, which senses the humidity and temperature from the surrounding. This sensor can measure a temperature ranges from 0 °C to 50 °C and humidity range from 20% to 90% with an accuracy of ±1 °C and ±1% [7]. It works within operating voltages of 3.5V to 5.5V and operating currents of up to 0.3mA. The DHT11 sensor module gives the measured value of the temperature in degree Celsius. When a room temperature increased by one-degree Celsius, the sensor generates a voltage of 10mV [8]. Fig.2 demonstrates the schematic diagram of the proposed system simulated by proteus software. For the cooling purpose, we connected the battery and the dc fan, relay switch, an NPN transistor in series and the base of the NPN transistor connected to a 10 KΩ resistor and Pin 6 of Arduino.

Meanwhile, Pin 2 of DHT11 connected to Pin 14 of the Arduino, while Pin 4 and Pin 1 are connected to GND and +5V power, respectively. However, Pin 3 has no connection (NC). The relay switches are used to control the power transmitted to the dc fan and the heater (lamp). The Liquid Crystal Display (LCD) was connected to the pin (13,12,11,10,22,20) of Arduino to display the data feed into the microcontroller and the output information. The value of the DHT11 sensor reading is displayed on the LCD screen every second. The potentiometer measures the voltage used by LCD. It has three connected pins, in which Pin1 connected to the ground, Pin 2 connected to 5V power, and Pin 3 connected to Pin 3 (V_{EE}) of LCD.

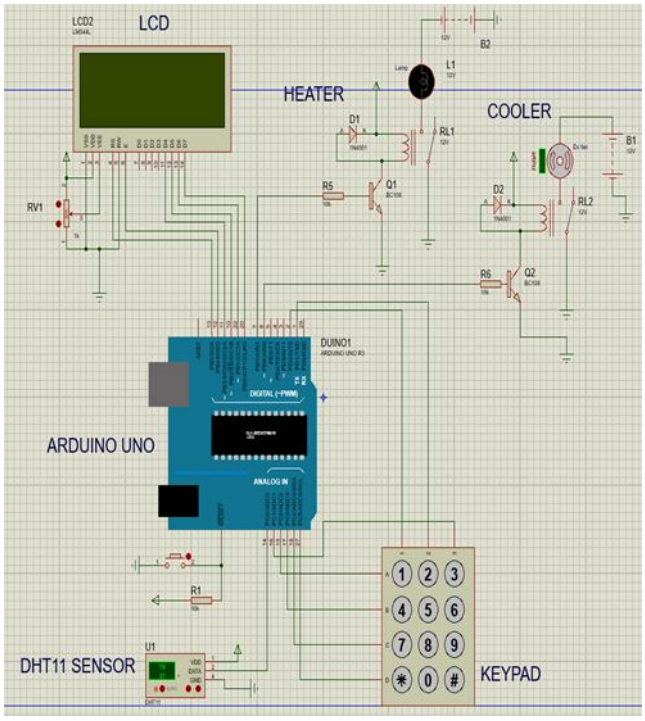


Fig.2 Schematic diagram of the proposed system simulated by proteus

2.1. Fan speed control system

The main technique to control the speed of Dc fan is called pulse width modulation (PWM) [4, 9]. The fan's speed will be controlled and monitored according to the number of duty cycles and Pulse Width Modulation (PWM). Because the pulse width modulation and amplitude of the pulse signal have a proportionality, then variable duty cycles are used. Duty cycle means a particular time that pulse width signal reached high during its operation. When the surrounding temperature changes, the fan speed control system uses various duty cycles from 0 to 100. That means the analogue-digital converter (ADC) writes various duty cycles to a Pin 6 of Arduino. These are 0%, 25%, 50%, 75%, and 100% duty cycles. Its corresponding fan speed is zero, slow, medium, fast, and very fast, according to the measured temperature [2,6].

2.2. Components used

The proposed system was composed of several circuit components. Table 1 below shows the name of the components and its specifications.

Table 1 The components and specification of materials used.

Name of Components	Description
Rectifier diode	1N4001
Resistors	10 KΩ
Relay switch	Two relay switches
Arduino	Arduino Uno R3
Humidity and Temperature sensor	DHT11 sensor
Transistor	BC108
Fan	DC fan
Heater	heater lamp
Keypad	3x4 Keypad
LCD	LM044L (20x4) LCD
Battery	12 volts battery
Potentiometer	POT-HG potentiometers

2.3. Software implementation

The code is written in an Arduino IDE and uploaded to the Arduino board through the USB cable connected to the computer [9]. In this work, we divided the program into two flowcharts; *flowchart 1* depicts the procedures to control the speed of the fan, and *flowchart 2* manifests how the entire system works.

2.3.1. Flowchart 1

Depending on the flowchart depicted in Fig.3, the speed of the fan is controlled, and the condition is executed only when the temperature difference is greater than zero.

$$\mathrm{T_d} = \mathrm{Ref.\,Temp_{max}} - \mathrm{Sensor\ Temp} \geq 0°\mathrm{C} \qquad (1)$$

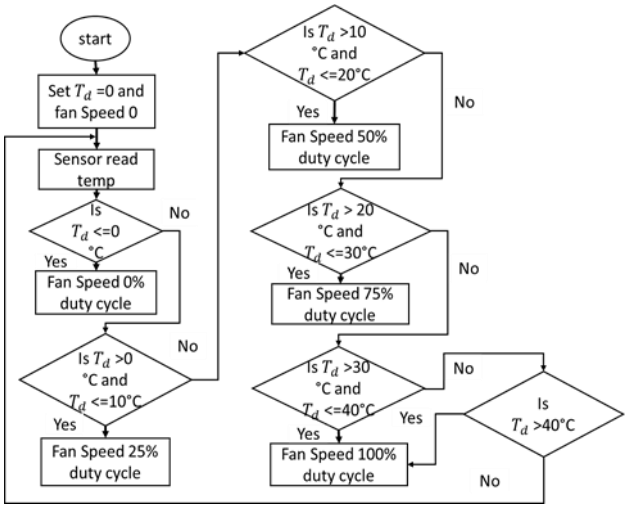


Fig.3 The flowchart for fan speed control

2.3.2. Flowchart 2

The flowchart in Fig.4 shows how the whole system works.

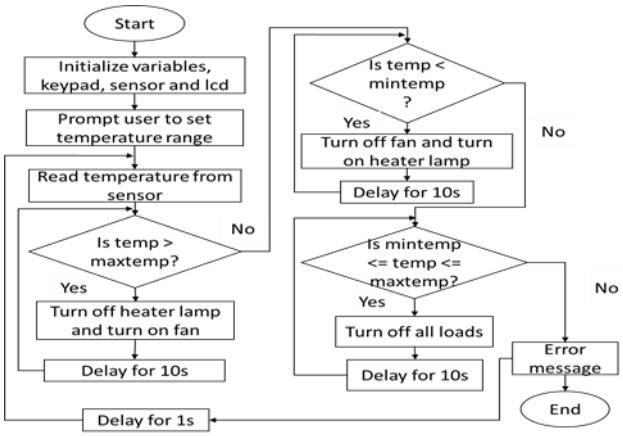


Fig.4 The flowchart shows how the entire system works

3. Result and Discussion

The system has been tested by setting up hardware components and using the Arduino program to execute the decoded instructions.

Fig.5 The hardware implementation of the proposed model

Firstly, when turned on the system, then it prompts the user to the input reference temperature, as shown in Fig.6. Then the user has set the minimum, and maximum reference temperature ranges as in Fig.6 (a).

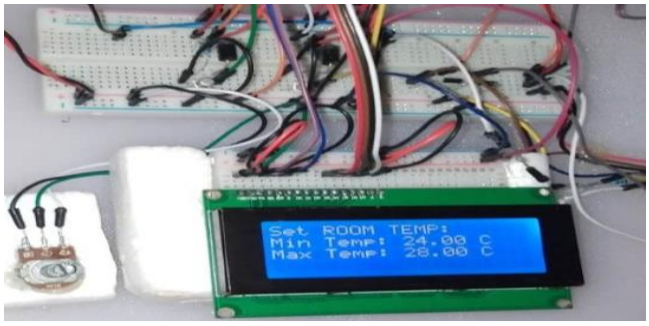


Fig.6 a)

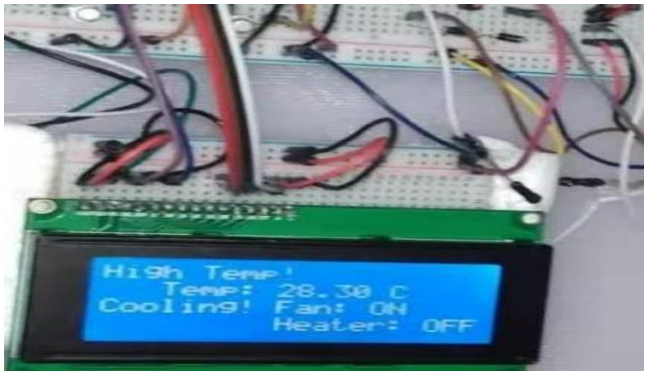


Fig.6 b)

Fig.6 (a) The user entered the minimum and the maximum reference temperature 24 and 28 °C, respectively, (b) the sensor reads the current room temperature 28.3 °C.

Fig.6 (b) sows that the sensor reads the current room temperature value of 28.30 °C. Here, the measured value of room temperature is higher than the maximum of the setpoint, so the fan is turned on, and the heater kept off until the condition changes.

This system is helpful for disabled persons and infants. It is applicable in areas such as manufacturing industry, computer server room, classroom, conference room, automobile to adjust the temperature automatically. This system's disadvantage is that it depends on the microcontroller, DHT11 sensor, heater, fan, and keypad to control and monitor the room temperature. If any of them got damaged, this system is interrupted. So, it is dependent on individual preferences. For this system to function correctly, we should make sure that the fundamental components are connected correctly and work properly.

4. Conclusions

In this paper, an automatic room temperature control system using Arduino and DHT11 sensor has been designed and constructed. The system used an Arduino microcontroller, keypad and DHT11 sensor to control and

monitor both the heater and the fan simultaneously. The DC fan is on when the room temperature is higher than the reference temperature, and its speed is controlled based upon the room temperature. When the room temperature is lower than the minimum of the reference temperature, then the heater lamp is turned on while the DC fan triggered off. When the room temperature is within the reference range, all the loads are automatically off. The main advantages of this system are for its low cost, ease of installation, simplicity, low power consumption, small size, and user-friendly. This project efficiently optimizes energy consumption in a room while keeping the room at a comfortable temperature.

Acknowledgements

We want to thank the University of Electronic Science and Technology of China, School of Mechanical and Electrical Engineering, Engineering Practicing Center for providing resources for implementing this project. Special thanks to Mrs Xiao Qian for giving all the support and guidance to complete this project.

References

[1] Dilruba Yamin, Automatic Room Temperature Controlled Fan Speed Controller Using PT100, International Journal of Scientific and Engineering Research, Volume 6, Issue 8, August 2015.

[2] M. Kumaran, I. Vikram, S. Kishore Kumar, R. Rajesh Kumar, S. Lokesh, Design of An Automatic Fan Speed Controlling System Using Arduino UNO. International Journal of Intellectual Advancements and Research in Engineering Computations, Volume-6 Issue-2, 2018 [2039-2042].

[3] Joseph Chuma, Design and Simulation of an Automatic Room Heater Control System, Botswana International University of Science and Technology, 2018.

[4] Siddika, S. F. Nasrin, Design, and Arduino-based Automatic Fan Control System Using PIR Sensor and LM35 Sensor. GSJ: Volume 6, Issue 8, August 2018.

[5] M. M. San, C. K. Win & K. Z. Mon, Design and Simulation of Fan Speed Control using Arduino UNO and LM35DZ, International Journal of Engineering Research and Advanced Technology (IJERAT), (E-ISSN: 2454-6135) Volume.6, Issue 6 June -2020.

[6] Suraj Kaushik, Automatic Fan Speed Control using Temperature and Humidity Sensor and Arduino, International Journal of Advance Research Ideas and Innovations in Technology Volume 2, Issue 8, 2018.

[7] Components101, January 5, 2018, DHT11 – Temperature and Humidity sensor, Available: https://components101.com/dht11-temperature-sensor, (Accessed November 4, 2020)

[8] Zairi Ismael Rizmam, Design an Automatic Temperature Control System for Smart Electric Fan Using PIC, International Journal of Science and Research (IJSR), Volume 2, Issue 9, September 2013.

[9] Biswajit Das, August 20, 2019, Temperature Based Fan Speed Control and Monitoring Using Arduino, https://www.electronicsforu.com/electronics-projects/fan-speed-control-monitoring-arduino

[10] AL Amoo, Design, and Implementation of a Room Temperature Control System: Microcontroller- Based, IEEE,2014.

EVALUATION METHOD OF SENSOR DATA CREDIBILITY BASED ON MULTI-SOURCE HETEROGENEOUS INFORMATION FUSION

HU JIXIONG, DUAN RUI, FENG YANLING, CHEN ZHUMING

School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
E-MAIL: jixionghu@std.uestc.edu.cn, duan_rui@uestc.edu.cn, yanlingfeng@std.uestc.edu.cn, zmchen@uestc.edu.cn

Abstract:

The reliability of sensor node data is crucial for data processing, especially sensor network data for security monitoring. However, existing evaluation methods cannot effectively evaluate the data credibility when the sensors are occluded or damaged. In order to solve this issue, a credibility assessment method for sensor data is proposed in this paper by fusing multi-source heterogeneous sensor data. Experimental results on mine smoke data show that the proposed method could effectively improve the veracity of evaluation when the sensors are disturbed or blocked.

Keywords:

Reliability; Sensor node; Multi-source; Information fusion; Evaluation

1. Introduction

Wireless sensor networks (WSN) are widely used in various fields at present. For example, in agricultural production, WSN is applied to monitor the growth environment and growth conditions of crops; in terms of industrial safety, WSN is used to monitor the safety of dangerous working environments such as coal mines, oil drilling, and nuclear power plants to ensure the safety of workers. However, due to the interference of many factors, sometimes the data collected by the sensor may not be true and credible, so the reliability of the sensor data must be evaluated.

For the credibility assessment of data, researchers have proposed a variety of research methods, Marsh [1] first designed a mathematical model for calculating credibility, and elaborated and defined credibility. Galland [2] developed a kind of fixed-point algorithm to evaluate the credibility of the data provided by the data source. Guo [3] et al. used a new method of estimating the credibility based on D-S evidence theory. M. Cao [4] et al. and Jikui Wang [5] et al. proposed a sensor data evaluation method based on Bayesian estimation. W. Gang, B. Zhang, Y. Zhang and others [6-8] combined BP neural network and fuzzy sets to fuse data. However, none of the above algorithms considers the relationship between data sources. In June 2019, Xinjian Wang [9] and others combined the correlation between data sources on the reliability evaluation of air quality sensor data, establishing a data credibility measurement model. However, the model cannot correctly evaluate the data when the sensors are occluded.

Therefore, in order to solve this problem, this paper studied a new method based on multi-source heterogeneous fusion through the fusion of multi-source heterogeneous sensor data around the sensor being evaluated.

2. Data credibility calculation

2.1. Definition of sensor data reliability

At present, there is no clear and accepted definition of the reliability of sensor data. Generally speaking, Credibility refers to the truth of the data [9], and then the reliability of sensor data can be thought to reflect the true state of the measured object in the expected environment. The expected environment refers to the target environment that is measured, for example, the smoke concentration in the room is measured by a sensor, but there is a situation where the sensor is covered by external objects, which results in the sensor data not reflecting the real smoke concentration in the room. That is, the true state of the expected environment cannot be correctly reflected. Untrusted data is divided into two categories in this paper: erroneous data and data in undesired environments. Among them, the error data is mainly caused by sensor failure, measurement error and various kinds of noise. Further, the data in the unexpected environment is mainly caused by the abnormal environment due to the sensor being obscured by external objects.

2.2. Calculation of sensor data credibility

In this paper, the credibility of the target sensor data is

comprehensively evaluated from two dimensions of time and space based on multiple sensors and multi types of sensors. The calculation formula of data credibility is as follows:

$$R_i^j = (K_{11}C_{tr}{}^j + K_{12}C_{ave}{}^j)(K_{21}F_i^j + K_{22}S_i^j)$$
$$\begin{cases} K_{11} + K_{12} = 1 \\ K_{11} > 0, K_{12} > 0 \end{cases} \quad (1)$$
$$\begin{cases} K_{21} + K_{22} = 1 \\ K_{21} > 0, K_{22} > 0 \end{cases}$$

In the formula, R_i^j is the credibility of the i-th data of sensor j; Firstly, $C_{tr}{}^j$ is the correlation between the historical trend of the data measured by sensor j and the historical trend of the surrounding sensor data; $C_{ave}{}^j$ is the clustering degree of the mean value of the data measured by sensor j relative to the mean value of the data from the surrounding similar sensors; Then, F_i^j is the credibility of the i-th data obtained according to the historical data of sensor j; S_i^j is the credibility of the i-th data of target sensor j after fusing multiple different types of sensor data .Finally, K_{11}, K_{12}, K_{21} and K_{22} are the weight factors .where $K_{11} + K_{12}$ = 1, $K_{21} + K_{22}$ = 1.

a） the definition of $C_{tr}{}^j$

$$C_{tr}{}^j = \frac{1}{n}\sum_{i=1}^{n}\left|r(Tr^i, Tr^j)\right| \quad (2)$$

Where r is the correlation function, Tr is the trend of historical data, and i is the adjacent sensor of sensor j.

b） the definition of $C_{ave}{}^j$

$$C_{ave}{}^j = \frac{1}{\left|\sum_{i=1}^{m}|V_j - V_i| * d_{ij} - \frac{1}{m}\sum_{i=1}^{m}\sum_{p=1}^{m}|V_i - V_p| * d_{ip}\right| + 1} \quad (3)$$

Where V_j is the historical data mean value of sensor j, i is the proximity sensor of sensor j, p is the proximity sensor of sensor i, and D is the distance factor between sensors.

c） the definition of F_i^j

$$\Delta f_i^j = |r_i - Sp_i| \quad (4)$$
$$F_i^j = \begin{cases} 1 & \Delta f_i^j \le \eta \\ \dfrac{3\eta - \Delta f_i^j}{2\eta} & \eta < \Delta f_i^j < 3\eta \\ 0 & \Delta f_i^j > 3\eta \end{cases} \quad (5)$$

Where, r_i is the i-th data measured by the sensor j, Sp_i is the predicted data based on the historical data of sensor j, and η is the threshold value of credibility evaluation .

d） the definition of S_i^j

$$\Delta s_i^j = | r_i - Mp_i | \quad (6)$$
$$S_i^j = \begin{cases} 1 & \Delta s_i^j \le \eta \\ \dfrac{3\eta - \Delta s_i^j}{2\eta} & \eta < \Delta s_i^j < 3\eta \\ 0 & \Delta s_i^j > 3\eta \end{cases} \quad (7)$$

Where, r_i is the i-th data measured by the sensor j, Mp_i is the predicted data based on the fusion of multiple heterogeneous sensors, and η is the threshold value of credibility evaluation.

3. Credibility evaluation model based on ARIMA and BP neural network

First of all, Autoregressive Integrated Moving Average model (ARIMA) model is uesd to analyze and predict the data of a single sensor to obtain the parameters Sp_i in Eq. 4, and calculate the credibility F_i^j in Eq. 1.

What is more, BP neural network combines the data of various heterogeneous sensors for predicting the data of the target sensor, and calculating the parameters Mp_i in Eq.6, so as to calculate the credibility S_i^j in Eq.1.

In particular ,when training the BP neural network, the $K_{22}S_i^j$ term should be removed in formula 1,where the coefficient K_{21} is set to 1; At last, High-confidence data(R_i^j >95%) is used as the initial training data of the BP neural network until the model training is completed.

Finally, Seasonal-Trend decomposition procedure based on Loess (STL) algorithm is applied to extract the trend Tr^j of the data of each sensor, and Tr^j is substituted into the Eq. 2 to calculate relevance of data trends $C_{tr}{}^j$, and then the outlier degree $C_{ave}{}^j$ of the data average is calculated through formula 3 according to the average value of the sensor data in the recent period. Finally, $C_{tr}{}^j$, $C_{ave}{}^j$, F_i^j, and S_i^j are substituted into formula 1 to calculate the current the credibility of the i-th data of sensor j(R_i^j).

4. experimental verification

In order to verify the effectiveness of the evaluation

model proposed in this paper, a set of roadway smoke simulation data sets based on pyrosim software were selected for testing, and the simulation results of the model were compared with those of Xinjian Wang et al.[9]

The data of a smoke sensor sd1 in the data set is selected as the target needed to be evaluated, and the noise and interference are added to the data manually to verify the ability of the model to evaluate the reliability of the data when the sensor is disturbed by noise and the sensor is blocked or damaged. The original data of sensor sd1 is shown in Figure 1, and the data of sensor sd1 after noise adding is shown in Figure 2.

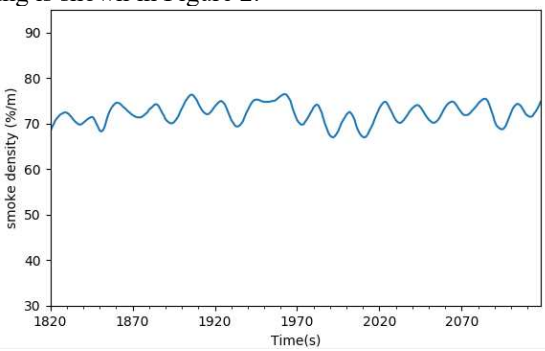


Fig.1 The raw data

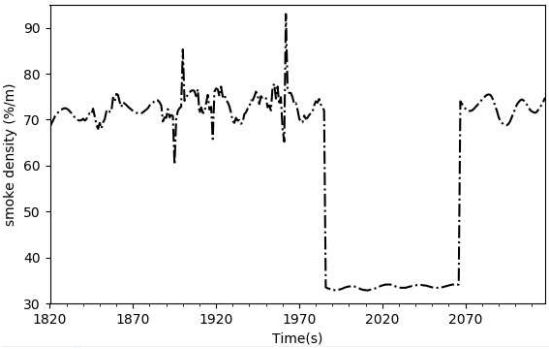


Fig.2 The data to be evaluated after adding noise

The data from 1820s to 1985s are the data after noise adding under non-occlusion condition, and the data from 1985s to 2068s are the data measured under occlusion; Figure 3 and Figure 4 are the smoke sensor data and temperature sensor data fused during the evaluation respectively, and then the noisy data are input into the model for assessment.

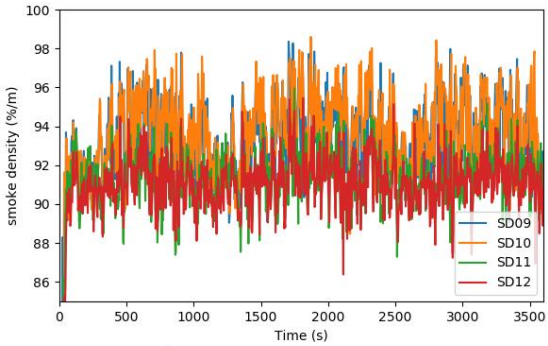


Fig.3 Partial smoke sensor data

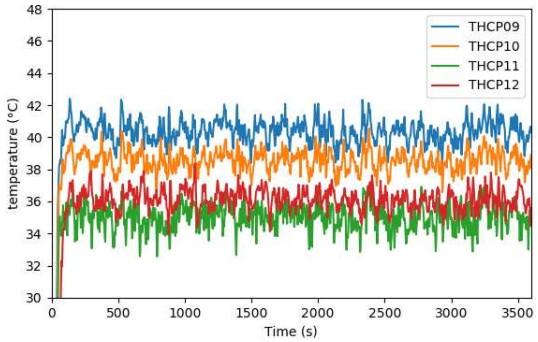


Fig.4 Partial temperature sensor data

The parameters of ARIMA model are determined as (3,0,1) by calculating Autocorrelation coefficient(ACF), Partial autocorrelation coefficient(PACF) and Augmented Dickey-Fuller test (ADF). The number of neurons in the hidden layer of BP neural network is 10, the number of layers is 5, and the learning rate is 0.01. The evaluation results are shown in Figure 5.

In Figure 5, the coordinates on the left are smoke concentrations and the coordinates on the right are confidence levels. Figure 5 shows that during the period from 1820s to 1837s, the credibility is 100%, which is due to the fact that the data is original data. At 1838s, the credibility began to change, especially in 1895s, 1899s, 1916s and 1961s, the credibility is very low; in the period from 1855s to 2067s, the credibility is 0% because the sensors are blocked, After 2067s, it is normal data, and the credibility of the data gradually rises to 100%. Compared with the simulation results of Xinjian Wang et al.[9] (see Figure 6), the proposed method can not only yield better results but also effectively evaluate the data when the sensor is occluded.

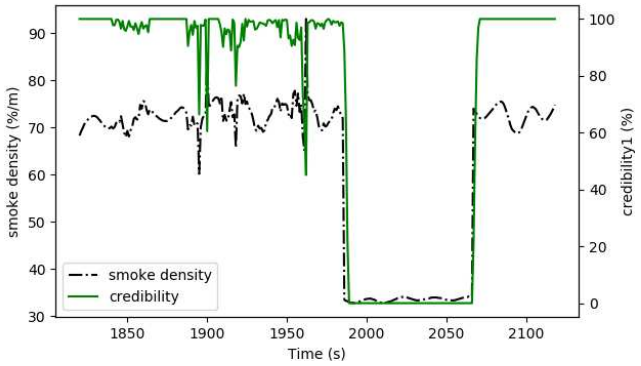


Fig.5 Evaluate the results

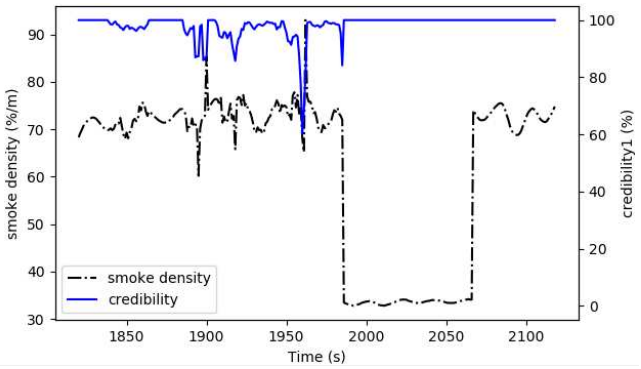


Fig.6 Evaluate the results

5. Conclusions

In this paper, a multi-source heterogeneous information fusion method based on ARIMA and BP neural network is proposed to evaluate the reliability of sensor data. By fusing the temporal correlation of the evaluated sensor data, the spatial correlation of similar sensor data, and the temporal and spatial correlation between different measured physical data, this method can effectively evaluate the data reliability of the sensor when it is masked, and also improve the evaluation effect of the data reliability when the sensor is not masked, providing a better evaluation method of data quality for big data processing.

Acknowledgment

This paper is Supported by the National Key Research and Development Project of China (2018YFC0808302).

References

[1] Marsh, Stephen Paul, Formalising Trust as a Computational Concept, University of Stirling, 1994.

[2] Galland A, Abiteboul S, Marian A, Corroborating information from disagreeing views, Proceedings of the third ACM international conference on Web search and data mining. ACM, 131-140, 2010.

[3] H. Guo, W. Shi and Y. Deng, "Evaluating Sensor Reliability in Classification Problems Based on Evidence Theory," in IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 36, no. 5, pp. 970-981, Oct. 2006, doi: 10.1109/TSMCB.2006.872269.

[4] M. Cao and D. You, "An application of optimized bayesian estimation data fusion algorithm in tire pressure monitoring system," 2018 Chinese Control And Decision Conference (CCDC), Shenyang, 2018, pp. 6564-6568, doi: 10.1109/CCDC.2018.8408284.

[5] J. K. Wang, Bayesian conflicting Web data credibility algorithm, Journal of Zhejiang University(Engineering Science), Vol.50, No.12, 2380-2385, 2016.

[6] W. Gang, L. Xiangyang, W. Guangen, G. Yong and M. Simin, "Research on Data Fusion Method Based on Rough Set Theory and BP Neural Network," 2020 International Conference on Computer Engineering and Application (ICCEA), Guangzhou, China, 2020, pp. 269-272, doi: 10.1109/ICCEA50009.2020.00065.

[7] B. Zhang, J. Lin, Z. Chang, X. Yin and Z. Gao, "The application of multi sensor data fusion based on the improved BP neural network algorithm," 2016 Chinese Control and Decision Conference (CCDC), Yinchuan, 2016, pp. 3842-3846, doi: 10.1109/CCDC.2016.7531655.

[8] Y. Zhang, P. Zhao, Z. Yan, M. Yang and B. Li, "The Research for A Kind of Information Fusion Model Based on BP Neural Network with Multi Position Sources and Big Data Selection," 2019 IEEE 2nd International Conference on Electronics Technology (ICET), Chengdu, China, 2019, pp. 619-623, doi: 10.1109/ELTECH.2019.8839458.

[9] X. Wang, X. Li, Y. Zhao, Y. Li and B. Zhang, "Credibility Analysis of Air Quality Data Based on Improved Measurement Method," 2019 Chinese Control And Decision Conference (CCDC), Nanchang, China, 2019, pp. 4421-4425, doi: 10.1109/CCDC.2019.8832967.

AN AUTOMATIC DATA CLEANING AND OPERATING CONDITIONS CLASSIFICATION METHOD FOR WIND TURBINES SCADA SYSTEM

ZHANG QUANLIN[1], ZHANG XIAOXIAO[1], HOU CHENGGANG[1]

[1]School of Mechanical Engineering, Xi'an Jiaotong University, Xi'an, 710049, China
E-MAIL: zhangquanlin@stu.xjtu.edu.cn, 820655017@qq.com, chghou@xjtu.edu.cn

Abstract:

The Supervisory Control and Data Acquisition (SCADA) system can provide significant information about the wind turbine health monitoring. However, the SCADA data contains enormous abnormal state data due to wind curtailment, equipment or sensor malfunction. In addition, complicated and constant changing operating conditions pose great challenges to effective and reliable fault detection. In this work, an automatic data cleaning and operating conditions classification approach is proposed. First, fundamental characteristics of different operating condition are analyzed according to control strategy, and data cleaning rules are constructed to remove abnormal state data. Then, change-point method is adopted to further clean residual abnormal state data that is stacked below the normal generation state data in the generator rotor speed-power curve. Second, the operating conditions classification criteria are constructed based on fundamental characteristics of different operating stages, and the classification parameter values are obtained adaptively according to data characteristics of different operating stages. Finally, the data cleaning and operating conditions classification approach is evaluated on the real-world SCADA dataset that was collected from a wind farm in East China. The results demonstrate that the proposed method can effectively distinguish normal power generation state data from abnormal power state data and realize operating conditions classification for different wind turbines automatically.

Keywords:

SCADA system; Data cleaning; Operating conditions classification; Control strategy; Change point detection

1. Introduction

As one of the cheapest sources of clean and renewable energy, wind power generation has developed rapidly over the past few decades [1]. However, wind turbine, especially the large-scale turbine, will be prone to fault due to poor manufacturing quality and harsh environment [2]. The operation and maintenance cost of wind turbines accounts for 25%-30% of the overall energy generation cost [3], which indicates that more effort need to make to reduce the operation and maintenance costs. As the most prevalent wind turbine condition monitoring system, SCADA system records comprehensive information of nearby all subcomponents, but these data have not been used effectively because of a large number of abnormal state data and complicated and ever-changing operating condition. Therefore, a data cleaning and operating conditions classification method need to be proposed to handle noisy SCADA data and improve the efficiency of data utilization.

SCADA data cleaning and operating conditions classification have attracted much research attention in academia and industry. To date, SCADA data cleaning methods can be roughly divided into the following three types. The first type of method directly uses programmable logic controller (PLC) codes to determine the operating conditions of wind turbines [4]. This method can effectively identify the downtime state data and start-up state data, but has limited ability to completely remove the power-limit state data. The second type establishes a mathematical model of wind power curve to remove abnormal data. Parametric [5-6] and non-parametric [7-8] methods are commonly used to model wind power curve, then the abnormal state data can be identified by using the approach of control charts. However, this type of methods requires a large number of normal power generation state data for training. The third type cleans abnormal data through the position distribution of the points in the wind power curve, including several implementation techniques like image processing [9-10] and clustering method [11-12]. These method cannot remove abnormal data that mixed in normal power generation data, and the performance of data cleaning depends heavily on the distribution of data.

The current operating conditions classification methods can be roughly divided into the following two types. The first type of method uses single parameters, for instant wind speed [13] or power [14], to classify the operating condition, which can simply achieve data classification but cannot effectively describe the complicated operating conditions of wind turbines. The second type of methods uses clustering

technique like K-means [15-16] or fuzzy C-means [17] to achieve the operating conditions classification. Despite the fact that these methods worked, the classification result is hard to explain due to the inherent deficiency of clustering algorithm.

In summary, SCADA data cleaning and operating conditions classification have been researched for many years, there are still some issues remains to date. Abnormal state data such as power-limit state data cannot be removed completely and it is not clear that physical interpretation of operating conditions classification results. In order to address these problems, this paper proposes a novel data cleaning and operating conditions classification framework. The proposed method analyzes the behavior characteristics of abnormal state and each normal stages based on control strategy, then data cleaning rules and operating conditions criteria are constructed according to these characteristics. Most of abnormal state data can be effectively removed by cleaning rules and residual power-limit state data by change point method. Due to the classification criteria are consistent with control logic, the classification results are more reliable and easier to explain.

2. Operating conditions of wind turbine

Wind turbine is a complex nonlinear electromechanical equipment. The operating conditions are complicated and ever-changing. The ideal performance curve is shown in Figure.1, According to this control strategy, the operating conditions can be divided into abnormal and normal power generation state.

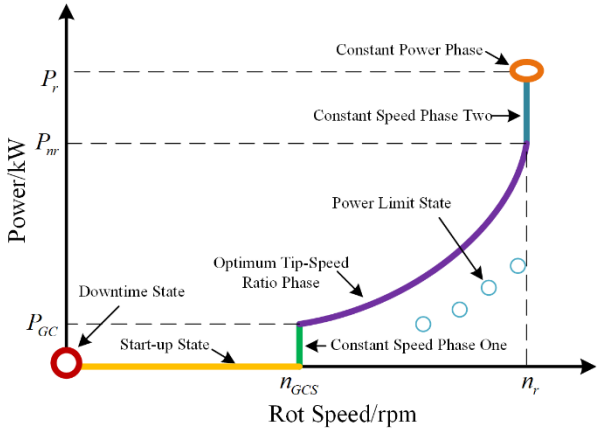


Fig.1 Operating conditions of wind turbines

2.1. Abnormal power generation state

The abnormal generation state refers to the output power is zero or does not conform to theoretical performance curve which includes downtime state, start-up state and power-limit state.

Downtime State. When suffering from equipment malfunctions or extreme environment, wind turbines will be shut down. In this state, the impeller of the wind turbine will stop rotating, the generator rotor speed n and the output power P will be zero.

Start-up State. When the self-inspection is completed and the wind speed meets the start-up requirements, the wind turbine will enter the start-up state. In this state, the blade angle decreases, the generator speed gradually rises from zero to the grid-connected speed. The output power P is near zero at this time, because the grid-connected condition is not reached.

Power-limit State. Due to wind curtailment or the temperature of a component is near the preset value. The output power P is limited by reducing the generator torque or increasing the blade angle to limit wind energy absorption. In this state, the blade angle is greater than 0.5.

2.2. Normal power generation state

The normal power generation state follows the theoretical performance curve which can reflect the actual performance of the turbine. According to control logic, it can be further divided into constant speed phase I, optimum tip-speed ratio phase, constant speed phase II and constant power phase.

Constant Speed Phase I. In this phase, the blade pitch angles are near zero, the generator rotor speed is controlled to keep near the grid-connected speed n_{GCS} by adjusting the generator torque. With the increase of the generator torque, the output power gradually increases to the maximum power P_{GC} at the grid-connected speed n_{GCS}.

Optimum Tip-speed Ratio Phase. In this phase, the blade pitch angles are near zeros, the torque of generator is adjusted according to the wind speed so as to track the optimum tip speed ratio to ensure the maximum wind energy can be captured. In this stage, the generation speed rises from grid-connected speed n_{GCS} to the rated speed n_r, and the output gradually rises from the maximum power P_{GC} at grid-connected speed n_{GCS} to the minimum power P_{nr} at the rated speed n_r.

Constant Speed Phase II. In this phase, the blade pitch angles are near zeros, the generator speed is kept near the rated speed n_r by adjusting the generator torque. With the increase of generator torque, the output power will gradually increase to the rated output power P_r.

Constant Power Phase. In this phase, it can keep the output power of the generator near the rated power through the dual regulation of the generator torque and the pitch angle.

When the wind speed exceeds the rated wind, the change of blade pitch angle is used to limit the absorption of wind energy, which can protect the wind turbine and ensure the stable output power.

3. Data cleaning and operating conditions classification

This section proposes a framework to accomplish data cleaning and operating conditions classification, the flow chart is shown in Figure 2. In the first part, data cleaning algorithms are developed to remove abnormal state data. The normal power generation state data can be obtained, and further be divided into four stages in the second part.

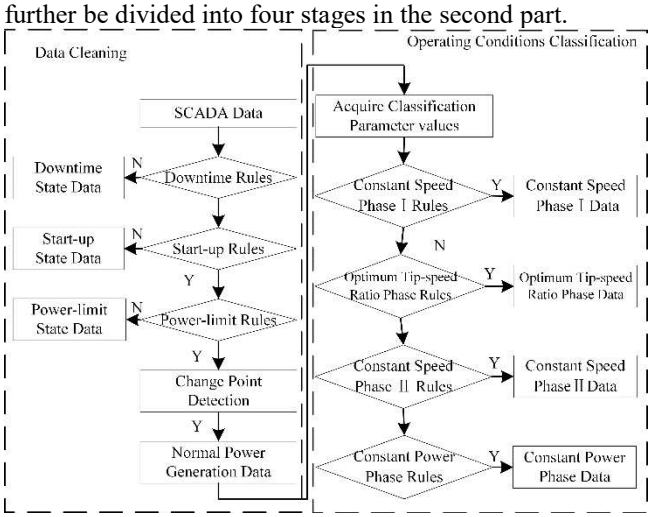


Fig.2 Flow chart of data cleaning and operating conditions classification.

3.1. Data cleaning

The primary purpose of data cleaning is to extract the normal power generation state data from raw SCADA data. The process of data cleaning can be separated into two steps including data cleaning by rules and further cleaning based on change point detection.

Step 1, Developing rules of data cleaning identifies and filters the abnormal state data. According to the theoretical analysis of control strategies mentioned in section 2, the fundamental characteristics of downtime state, start-up state and power-limit state are acquired. The cleaning rules are constructed in combination with data characteristics and PLC code as shown in Table 1. Abnormal state data can be identified and removed based on these rules successively.

Step 2. Data after primary cleaning may contain partial power-limit state data as shown in Figure 3. These abnormal state data are caused by directly limiting the generator torque rather than adjusting pitch angle, therefore, they cannot be removed by power-limit rules. The residual power-limit state data stacks below normal generator state data, the power of power-limit state changes suddenly relative to normal power generation state, so it is feasible to adopt change point detection to further remove residual abnormal data [18]. There are many way to implement change point detection including bayesian method, least square method, maximum likelihood method and local comparison method [19]. Here, the least square method is adopted to identify the change point location because it has the advantages of not assuming a distribution of random errors.

Table 1 Rules of data cleaning.

Operating State	Fundamental characteristics
Downtime	$n = 0,\ P = 0$, PLC code = 3, 4, 5, 6
Start-up	$v_{cut-in} \le v \le v_{cut-out},\ P \le 0,$ $0 \le n \le n_{GCS}$, PLC code = 1
Power-limit	$v_{cut-in} \le v \le v_{cut-out},\ 0.5 \le \beta,$ $n_{GCS} \le n \le n_r,\ 0 \le P \le P_r$

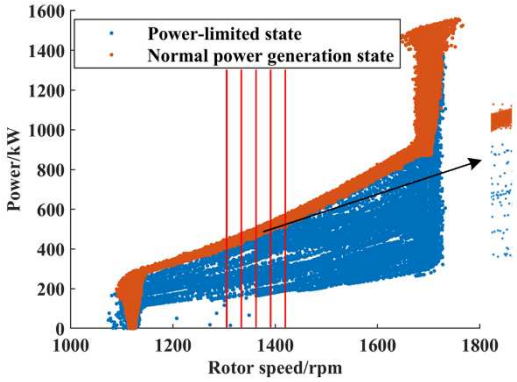


Fig.3 Equal interval partition of rotor speed.

The generator rotor speed is divided at equal intervals of 1 rpm as shown in Figure.3 and the data samples set D of a certain rotor speed interval is obtained.

$$D = \{(n_1, p_1),\ (n_2, p_2),\ \cdots,\ (n_k, p_k)\} \quad (1)$$

Where n_i is the generator rotor speed, P_i is the power.

The power series P is arranged in a descending order without duplicate values.

$$P = \{P_1,\ P_2,\ \cdots,\ P_m\} \quad (2)$$

The variance of each points for power series is

$$\sigma_j = \frac{\sum_{i=1}^{j} \left(P_i - \overline{P}_i\right)^2}{j} \quad (3)$$

Where σ_j is the variance of the first j points, P_i is the power value of the j-th point, and $\overline{P}_i$ is the average power of the first i points.

Due to the power series of normal power generation state data is aggregated in a small region, the variance of

power series before the change point increases slightly, and power-limit data stacks below normal generator state data, the variance of each point for power series after the change point changes greatly. So the entire variance series can be represented by two linear segments as shown in Figure.4, so linear regression model is used to fit the variance series.

$$\sigma_i = \begin{cases} \alpha^{(1)} + \beta^{(1)} i + e_i, & 1 \le i \le j \\ \alpha^{(2)} + \beta^{(2)} i + e_i, & j \le i \le n \end{cases} \quad (4)$$

Where $(\alpha^{(1)}, \beta^{(1)})$ and $(\alpha^{(2)}, \beta^{(2)})$ are regression coefficients, e_i is the difference between theoretical value and observed value, J is the change point.

According to the principle of least square method, the objective function is the sum square of e_i.

$$S_j = \sum_{i=1}^{j} \left(\sigma_i - \alpha^{(1)} - \beta^{(1)} i\right)^2 + \sum_{i=j+1}^{m} \left(\sigma_i - \alpha^{(2)} - \beta^{(2)} i\right)^2 \quad (5)$$

The change point J can be found by minimized S_j.

$$J = \arg\min_j S_j = \arg\min_j \left(\sum_{i=1}^{j} \left(\sigma_i - \alpha^{(1)} - \beta^{(1)} i\right)^2 + \sum_{i=j}^{n} \left(\sigma_i - \alpha^{(2)} - \beta^{(2)} i\right)^2 \right) \quad (6)$$

The data after change point J is considered as power-limit state data that should be removed.

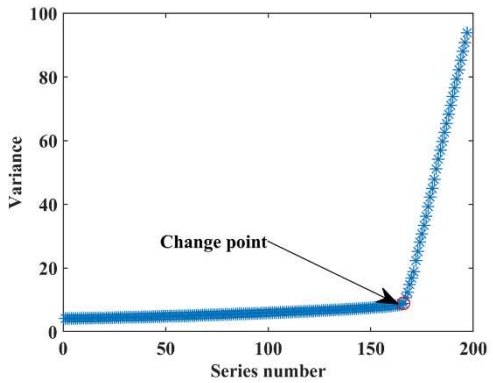


Fig.4 Variance of each point for power series.

3.2. Operating conditions classification

After data cleaning, the normal power generation state data is obtained, which can be divided into four stages. The specific process is shown in the right part of Figure.2. According to the fundamental characteristic mentioned in section 2, the criteria of operating conditions classification are constructed as shown in Table 2.

Unfortunately, boundary values between the four operating stages are changed with control strategy, as shown in Figure.5. Therefore, in order to accurately classify operating conditions, it is necessary to obtain the classification parameter values adaptively for different wind turbines. It can be figure out that the difference of parameter values of operating condition are mainly concentrated on the grid-connected speed n_{GCS}, the rated speed n_r, the maximum power P_{GC} at grid-connected speed, the minimum power P_r at rated speed.

Table 2 Criteria of operating conditions classification.

Operating Stage	Behavior of each stage
Constant Speed phase I	$n \le n_{GCS},\ \beta \le 0.5,$ $0 \le P \le P_{GC}$
Optimal Tip-Speed Ratio phase	$n_{GCS} < n < n_r\ ,\beta \le 0.5,$ $P_{GC} \le P \le P_{nr}$
Constant Speed phase II	$n_r \le n,\ \beta \le 0.5,\ P_{nr} \le P < P_r$
Constant Power phase	$n_r \le n,\ \ 0.5 < \beta,\ \ P_r \le P,$

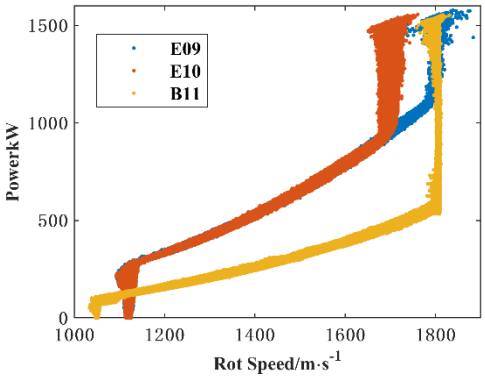


Fig.5 Rotor speed-power curves of different wind turbines.

According to wind turbine control strategy, there will be two peaks in the probability distribution of rotor speed correspond to constant speed phase I and constant speed phase II respectively as shown in Figure.6(a) [20]. According to this characteristic, the classification parameter values of rotor speed n_{GCS} and n_r can be determined by setting a threshold. The threshold can be set to the maximum value of probability distribution in the range of 100 to 200 above minimum rotor speed or below maximum rotor speed. It is obvious from Figure.4 that the derivative of rotor speed with respect to the power at different operating stages are different. Analogous to wind power curve, the rotor speed power curve can be acquired based on binning technique. The bin width is 1kW and average rotor speed can be obtained from each bin. Then the derivative of average rotor speed with respect to the power is calculated as shown in Figur.6(b). It can be figure out that the derivative of constant speed phase I and constant speed phase II tend to zero, while optimal tip-speed ratio phase is much larger than zero. According to this characteristic, the operating condition parameter values of power P_{GC} and P_{nr} can be acquired automatically. After

acquiring classification parameter values, the normal power generation state data can be divided into four stages according to the criteria shown in Table 2.

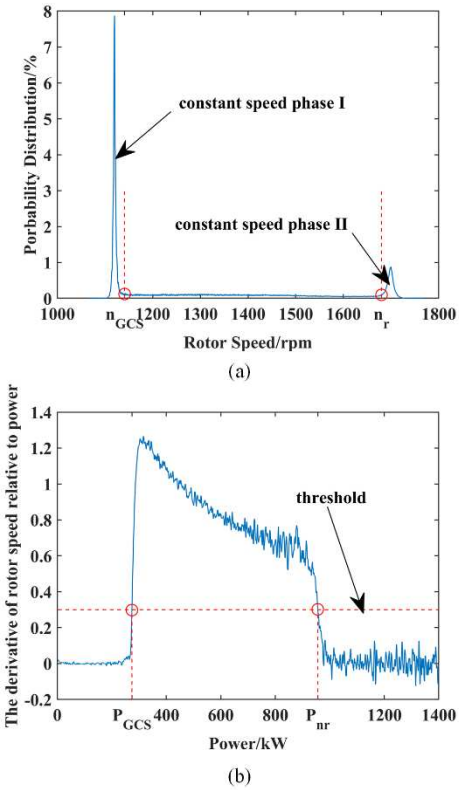


Fig.6 Automatically obtaining classification parameter values. (a) The probability distribution of rotor speed. (b) The derivative of rotor speed with respect to the power.

4. Case study

In order to examine the feasibility of the proposed method in this paper, the SCADA data was collected from real world doubly-fed wind turbines that locates at a wind farm in East China. The rated power is 1.5MW, the cut-in wind speed is 2.5 m/s, the cut-out wind speed is 25 m/s. The SCADA system records wind speed, generator rotor speed, power, PLC code and other parameters with sampling rate of 1Hz. In this paper, three turbines with typical abnormal data are selected for verify the proposed method, turbine 1 includes a large amount of stacked power-limit state data, turbine 2 contains some discrete power-limit state data while turbine 3 only contains some outliers. The results after data cleaning process are shown in Figure.7, it can be seen that abnormal data can be removed effectively especially for power-limit state data. Comparing with the raw SCADA data, the data after cleaning is closer to ideal rotor speed-power curve.

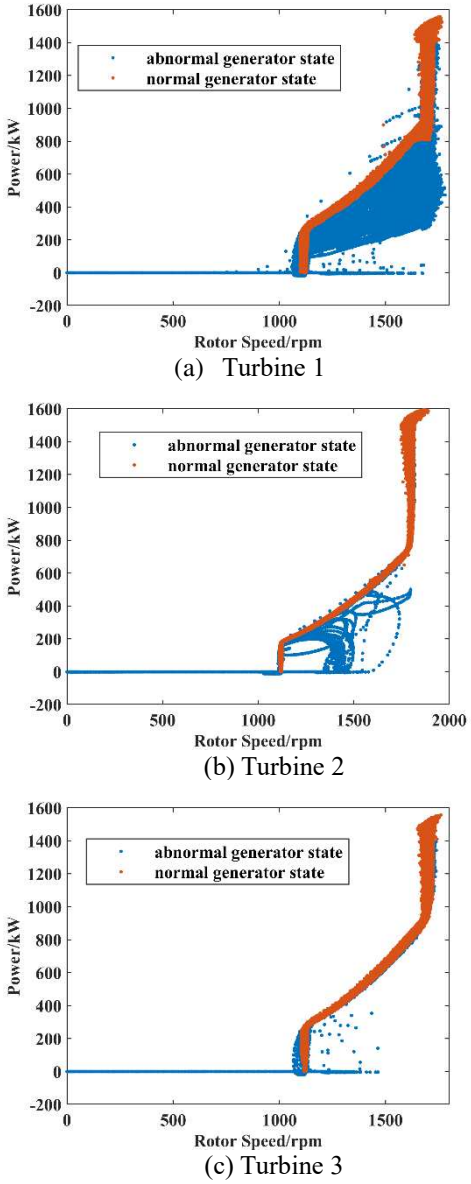


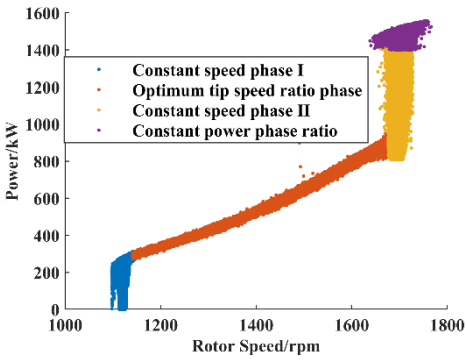
Fig.7 Results of data cleaning. (a) Turbine 1(b) Turbine 2 (c) Turbine 3

The normal power generation data can be obtained after data cleaning. The operating condition classification parameter values of three wind turbines are acquired automatically as shown in Table 3. Then, normal power generation state data were divided into four stages based on criteria in Table 2, the results are as shown in Figure.8(a) (b) (c). It can be inferred that the proposed method in this paper can achieved the operating conditions classification automatically for different wind turbines. In order to further

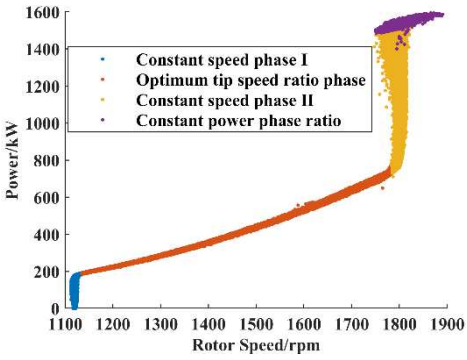
illustrate the effectiveness of the algorithm, operating condition classification based on fuzzy C-means (FCM) for turbine 3 is used for a comparative analysis and the result is shown in Figure.8(d). As a typical clustering algorithm, FCM can classify operating conditions in terms of wind speed, rotor speed and blade angle, but the results of each clustering are hard to interpret. Comparing to FCM, the classification results of the method proposed in this paper are consistent with control strategy and easier to explain.

Table 3 Parameter values of operating conditions classification.

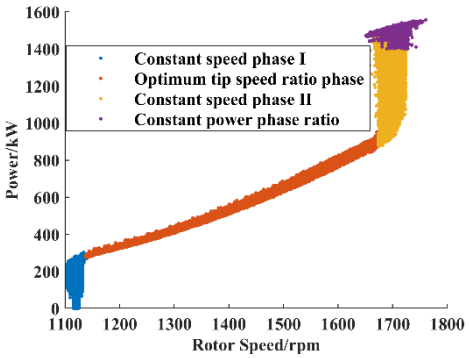
Parameters	turbine 1	turbine 2	turbine 3
n_{GCS}	1141	1135	1138
n_r	1677	1785	1674
P_{GC}	273.6	182.9	273.5
P_r	956.4	772.1	957.1



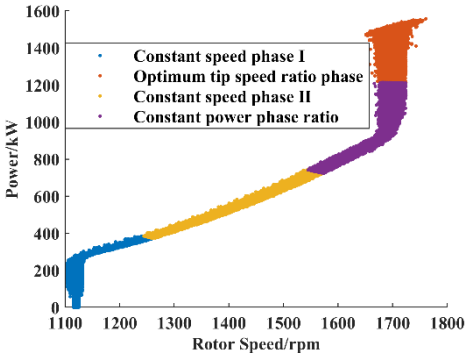
(a) Turbine 1



(b) Turbine 2



(c) Turbine 3



(d) Turbine 3

Fig.8 Results of operating condition classification. (a) (b) (c) Operating conditions classification based on classification criteria proposed in this paper for three turbines. (d) Operating conditions classification based on FCM for turbine 3.

5. Conclusions

The raw SCADA data of wind turbine contains a large amount of abnormal data and operating conditions are complex and ever-changing. In order to address these issues, this paper proposes a generic framework of data cleaning and operating conditions classification framework based on control strategy. Our method summarizes fundamental characteristics of operating conditions and constructs data cleaning rules and operating conditions classification criteria by analyzing a generic control strategy of wind turbine. Beside, change point detection is introduced to further remove the residual abnormal state data. Several real-world scenarios are used to verify the effectiveness of the proposed method, the experimental results demonstrate the proposed method can efficiently eliminate abnormal state data especially for power-limit state data. Compared with the fuzzy C-means clustering algorithm, the proposed method can classify the normal power generation data into four

operating stages in a reasonable way automatically for different wind turbines. The classification results conform to control logic and are easier to explain.

Acknowledgements

This research is partially funded by the National Natural Science Foundation of China, grant number 51675419.

References

[1] Ohlenforst K, Sawyer S, Dutton A, et al. Global wind report 2018. Global Wind Energy Council, Brussels, 2019.

[2] Ribrant J, Bertling L. Survey of failures in wind power systems with focus on Swedish wind power plants during 1997-2005. 2007 IEEE power engineering society general meeting. IEEE, 2007: 1-8.

[3] Milborrow D. Operation and maintenance costs compared and revealed. Wind Stats, 2006, 19(3): 3.

[4] Wei L, Qian Z, Yang C, et al. Pitch fault diagnosis of wind turbines in multiple operational states using supervisory control and data acquisition data. Wind Engineering, 2019, 43(5): 443-458.

[5] Kusiak A, Zheng H, Song Z. On-line monitoring of power curves. Renewable Energy, 2009, 34(6): 1487-1493.

[6] Carrillo C, Montaño A F O, Cidrás J, et al. Review of power curve modelling for wind turbines. Renewable and Sustainable Energy Reviews, 2013, 21: 572-581.

[7] Ciulla G, D'Amico A, Di Dio V, et al. Modelling and analysis of real-world wind turbine power curves: Assessing deviations from nominal curve by neural networks. Renewable energy, 2019, 140: 477-492.

[8] Lydia M, Selvakumar A I, Kumar S S, et al. Advanced algorithms for wind turbine power curve modeling. IEEE Transactions on sustainable energy, 2013, 4(3): 827-835.

[9] Long H, Sang L, Wu Z, et al. Image-based abnormal data detection and cleaning algorithm via wind power curve. IEEE Transactions on Sustainable Energy, 2019, 11(2): 938-946.

[10] Su Y, Chen F, Liang G, et al. Wind Power Curve Data Cleaning Algorithm via Image Thresholding*. 2019 IEEE International Conference on Robotics and Biomimetics (ROBIO). IEEE, 2019: 1198-1203.

[11] Zheng L, Hu W, Min Y. Raw wind data preprocessing: a data-mining approach. IEEE Transactions on Sustainable Energy, 2014, 6(1): 11-19.

[12] Yesilbudak M. Partitional clustering-based outlier detection for power curve optimization of wind turbines. 2016 IEEE International Conference on Renewable Energy Research and Applications (ICRERA). IEEE, 2016: 1080-1084.

[13] Becker E, Poste P. Keeping the blades turning: condition monitoring of wind turbine gears. Refocus, 2006, 7(2): 26-32.

[14] Tingting Y, Yang B, Weichun G, et al. Early Warning Method for Power Station Auxiliary Failure Considering Large-Scale Operating Conditions. 2019 IEEE 2nd International Conference on Power and Energy Applications (ICPEA). IEEE, 2019: 11-16.

[15] Dong Y, Li Y, Cao H, et al. Real-time health condition evaluation on wind turbines based on operational condition recognition. Proceedings of the CSEE. 2013, 33(11): 88-95.

[16] Wang H, Wang H, Jiang G, et al. Early fault detection of wind turbines based on operational condition clustering and optimized deep belief network modeling. Energies, 2019, 12(6): 984.

[17] Liu C L, Yan X. Monitoring of the State of the Gear Box of a Wind Power Generator Unit Based on the Operating Condition Identification. Journal of Engineering for Thermal Energy and Power. 2016, 31(07):41-46+133.

[18] Shen X, Fu X, Zhou C. A combined algorithm for cleaning abnormal data of wind turbine power curve based on change point grouping algorithm and quartile algorithm. IEEE Transactions on Sustainable Energy, 2018, 10(1): 46-54.

[19] Chen X R. Introduction to statistical analysis of change points. Journal of Applied Statistics and Management, 1991, 000(002):52-59.

[20] Ha J M, Oh H, Park J, et al. Classification of operational conditions of wind turbines for a class-wise condition monitoring strategy. Renewable energy, 2017, 103: 594-605.

RESEARCH ON PUBLIC OPINION DISSEMINATION MODEL AND COUNTERMEASURES

HOU GUANGWEI[1], QIU JIANFENG[2], YAN HAI [2]

[1]Innovation Center, University of Electronic Science and Technology of China, Chengdu 611730, China
[2]Information Science and Technology Institute, Zhengzhou 450000, China
E-MAIL: zxhgwwork@163.com, q471745920@126.com, 798853007@qq.com

Abstract:

With the maturity of information technology year by year, the information technology such as communication, network and media is developing unprecedentedly. In order to improve the guidance and control of network public opinion, the research of public opinion control has attracted more and more attention. In this paper, based on the theory of differential equation, the general principles of mechanism analysis and parameter identification are used to establish the model. This paper studies the dissemination law and effect of positive information and negative information under normal conditions. By controlling the model parameters, it reasonably analyzes and puts forward the active strategy of effective control of public opinion information. According to the specific situation of the confrontation conditions, the model is expanded to make it more in line with the actual situation under the confrontation conditions. Finally, through the obtained model, the practical significance of each parameter is analyzed, which proved some theoretical support for the government's decision making in public opinion control.

Keywords:

Public opinion information; Dissemination law; Dissemination effect; Differential equation

1. Introduction

With the development of Internet, the network is becoming the main way for citizens to express themselves, and the voice of different groups is more and more concerned by the public [1]. Nowadays, the proportion of new media exposure is still high, which is becoming an important way to affect public opinion. In this case, the pressure of public opinion control is increasing, and the research of public opinion is heating up day by day [2].

At present, for the study of the dissemination law of public opinion, one kind of the methods is the bottom-up modeling methods [3], which pays attention to the evolution of network public opinion with mutual influence among individuals. These models include: A series of cellular automata models for public opinion dissemination [4-5] represented by Sznajd model [6]; small world networks [7] represented by NW model [8], and the agent-based models show the trend of public opinion dissemination through the interaction of agents [9]. These models study the simple interaction rules between individuals, but they can't simulate the real world well.

The other kind of the methods is the top-down modeling methods [3], which pays attention to the evolution of network public opinion at the angle of groups. These models include epidemic model. Sudbury is the first to use SIR model [10] of epidemic model to study the spread of rumors [11]. The work represented by paper [12] uses SIS model [10] to simulate the dissemination of network public opinion, and the work represented by paper [13] introduces immune individuals and use SIR model to simulate the network public opinion dissemination. The epidemic models based on differential equation can describe the process of public opinion dissemination with time accurately, analyze its dissemination law, predict its characteristics and give its control methods.

In this paper, we extend SIR model. There are ignorant and known, and the known are divided into spreaders, no-spreaders and the stifler [14]. And according to positive and negative information, the paper establishes the transformation relationship; on this basis, media is introduced [15]. Considering the media and the known interaction stage, we introduce the immune rate and the awakening rate to describe the internal relationship of each factor [14]. Moreover, considering the confrontation condition [15], we make reasonable assumptions to expand the confrontation model, then define the Information Reliability, Personal Reliability, Repetition and establish the relationship between them. Through studying the differential equation of one side, the total number equation of one side's public opinion supporters is obtained, and the function of various factors in the confrontation condition is analyzed.

Based on the above two models, the paper combines the

meaning of each parameter and measures to influence the change of parameters, thus achieving the purpose of influencing the total number of public opinion supporters of one side. Combined with the model, the paper puts forward the strategies of realizing social security in normal conditions and in confrontation conditions to control the initiative.

2. System model

In our system model, there are ignorant (who don't know the news) and known. Among the known, there are spreaders (who will spread to the ignorant after knowing the news), no-spreaders (who will not spread after knowing the news), and the stifler (who know but do not believe) [14]. In the positive information dissemination model, it is assumed that the stifler is negligible and there exists no-spreader. In the negative information dissemination model, it is assumed that there is no no-spreaders and the known will be transformed into the stifler.

In the information dissemination model of the confrontation condition [15], it is assumed that there are only three types of people in the crowd: the ignorant, the information supporters of A and the information supporters of B. Here, the information supporters are assumed to be the spreader. Then we define Personal Reliability, Information Reliability, Repetition and establish a relationship between the three， and reclassify the population according to the difference of Personal Reliability.

Because Personal Reliability in different information will be different, we make a hypothesis on the information reliability of both sides. If Personal Reliability A is positive value, the one is the supporter of information A, or else he is a supporter of information B. The absolute value of the value is the Personal Reliability value. In this paper, we establish the general differential equation of the people whose personal reliability is p, and then sum them to get the total number of supporters of information A, that is, the total number of people affected by information A.

2.1. Basic Notation

In our system model, the total number of people N remained unchanged. The proportion of the ignorant, the known, spreaders, the stifler in the total number of people are $w(t)$, $y(t)$, $s(t)$, $i(t)$ respectively when time is t. Suppose there are two ways of information dissemination, one is media, the other is person. The number of media dissemination and personal dissemination are k, λ per day. The probability that the known become spreader is α; the probability that the known become no-spreader is β; the probability that the known become the stifler is γ; the probability that the ignorant become the stifler is η; the probability that the spreader become the stifler is μ.

To facilitate the expansion of the model, the following definitions are made：

Definition 1: The number of times an individual receives the same information is called Repetition to the individual.

Definition 2: Once the spread of information is accepted, there is a degree of recognition. We call it Information Reliability. Suppose that the theoretical credibility of information A is P_A, and that of B is P_B.

Definition 3: The degree to which a group of people believe in information is called Personal Reliability. People who believe in A are labeled A_i and have A_i $(i = 1,2,\ldots)$. The same is true for B. for example, Suppose the Information Reliability of A is 3, and an ignorant person accepts the A once, and the Personal Reliability is 3, which is one of the A_3.

2.2. Framework Overview

According to the hypothesis, The transformation relationship among the ignorant, the known, spreader, no-spreader and stifler is shown in the figure:

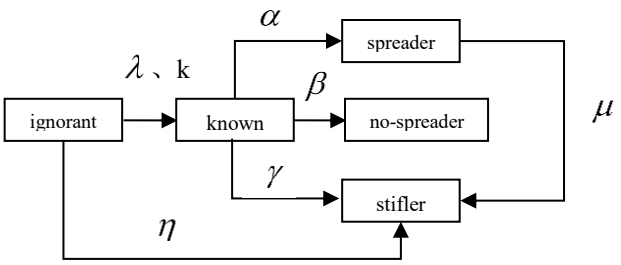


Fig.1 The transformation relationship of the five

As for the transmission of positive information, because it is easy to believe the positive information, it is assumed that the number of the stifler is ignored. Then the overall conversion diagram is:

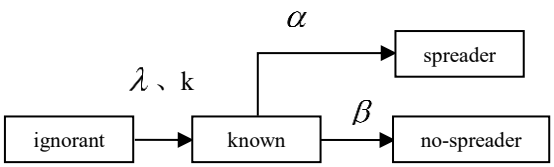


Fig. 2 The transmission of positive information

According to the hypothesis, each the known can make $\lambda w(t)$ ignorant into the known every day, and the media can make $kw(t)$ ignorant into known every day. There are $\lambda N w(t) y(t) + kw(t)$ ignorant receiving information every day. The known has the probability α to become the

spreader, so $\alpha(\lambda \mathrm{N}wy + \mathrm{k}w)$ is the increase rate of the number of the known Ny.

$$\mathrm{N}\frac{dy}{dt} = \alpha(\lambda Nwy + kw) \quad (1)$$

Because $\mathrm{w(t)} + \mathrm{y(t)} = 1$, and note that the ratio of known initial time (t = 0) is y_0, we have:

$$\frac{dy}{dt} = \alpha[\lambda y(1-y) + \frac{y}{N}((1-y)], y(0) = y_0 \quad (2)$$

Since people know that negative information will be stifler if they don't spread it, so the number of no-spreader is ignored. Because the known will become the spreader and the stifler, so we can simplify the process of the ignorant into the known. Then the transformation diagram is as follows [14]:

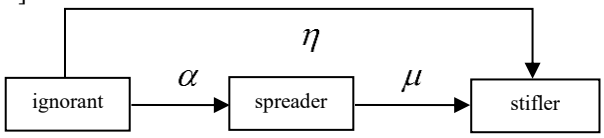


Fig.3 The transmission of negative information

On the one hand, if the number of spreader is s, $\alpha(\lambda \mathrm{N}wy + \mathrm{k}w)$ is the number of ignorant who become spreader, and $\mathrm{N}s\mu$ is the number of spreader who become stifler:

$$\mathrm{N}\frac{ds}{dt} = \alpha(\lambda Nwy + kw) - Ns\mu \quad (3)$$

On the other hand, $-(\lambda \mathrm{N}wy + \mathrm{k}w)$ is the change in the number of ignorant who receive information first and then become spreader and stifler, and $-\mathrm{N}w\eta$ is the change of the number of ignorant who have not received information and become stifler directly:

$$\mathrm{N}\frac{dw}{dt} = -(\lambda Nwy + kw) - Nw\eta \quad (4)$$

Because $\frac{dw}{dt} + \frac{ds}{dt} + \frac{di}{dt} = 0$, the change rate of the number of stifler is obtained:

$$\mathrm{N}\frac{di}{dt} = (\lambda Nwy + kw)(1-\alpha) + Ns\mu + Nw\eta \quad (5)$$

Based on the above analysis, the negative information dissemination model is obtained:

$$\frac{ds}{dt} = \alpha\left(\lambda wy + \frac{k}{N}w\right) - s\mu, y(0) = y_0 \quad (6)$$

$$\frac{dw}{dt} = -\left(\lambda wy + \frac{k}{N}w\right) - w\eta, w(0) = w_0 \quad (7)$$

$$\frac{di}{dt} = \left(\lambda wy + \frac{k}{N}w\right)(1-\alpha) + s\mu + w\eta, i(0) = i_0 \quad (8)$$

The following part will discuss the model of mutual offset between supporters of both sides in the case of the confrontation condition.

First of all, we make the following assumptions about the model:

1. Suppose A and B fight for public opinion, then the persons can only identify with the information of A or B at a moment.

2. Suppose that those who believe in A will become the spreader s_1 of A, and those who believe in B will become the spreader s_2 of B.

3. Suppose that the proportion of the ignorant to the total number of people is Nw, the proportion of people who believe in A to the total number of people is $\mathrm{N}s_1$, the proportion of people who believe in B in the total number of people is $\mathrm{N}s_2$, the number of people who communicate effective spreaders every day in the media of A is k_1, about B is k_2, the number of daily effective spreaders of s_1 is λ_1, and the number of daily effective spreaders of s_2 is λ_2.

4. Suppose that the ignorant may believe in A or B, and the people who believe in A will be confused by the information of B, so they don't know which side to believe and become the ignorant again. The same is true for those who believe in B.

The mutual transformation relationship is shown in the figure about ignorant, spreader s_1, spreader s_2:

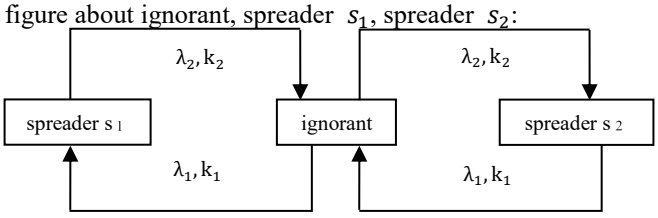


Fig.4 The transformation relationship of the three

For the spreader s_1 who believe in A, $\mathrm{N}w\lambda_1 s_1 + k_1 \mathrm{w}$ is the number of ignorant to spreader s_1, and $\mathrm{N}\lambda_2 s_1 s_2 + k_2 s_1$ is the number of people who are affected by B and become confused and become ignorant. For the spreaders s_2 who believe in B, $\mathrm{N}w\lambda_2 s_2 + k_2 \mathrm{w}$ is the number of ignorant to spreader s_2, and $\mathrm{N}\lambda_1 s_1 s_2 + k_1 s_2$ is the number of people who are influenced by B and become ignorant.

$$\mathrm{N}\frac{ds_1}{dt} = (\mathrm{N}w\lambda_1 s_1 + k_1 \mathrm{w}) - (\mathrm{N}\lambda_2 s_2 s_1 + k_2 s_1) \quad (9)$$

$$\mathrm{N}\frac{ds_2}{dt} = (\mathrm{N}w\lambda_2 s_2 + k_2 \mathrm{w}) - (\mathrm{N}\lambda_1 s_1 s_2 + k_1 s_2) \quad (10)$$

Since $\frac{dw}{dt} + \frac{ds_1}{dt} + \frac{ds_2}{dt} = 0$, we can know the change of the number of ignorant:

$$\mathrm{N}\frac{dw}{dt} = (\mathrm{N}\lambda_2 s_1 s_2 + k_2 s_1) + (\mathrm{N}\lambda_1 s_1 s_2 + k_1 s_2) - (\mathrm{N}w\lambda_1 s_1 + k_1 \mathrm{w}) - (Nw\lambda_2 s_2 + k_2 w) \quad (11)$$

So we have:

$$\frac{ds_1}{dt} = \left(\mathrm{w}\lambda_1 s_1 + \frac{k_1}{N}\mathrm{w}\right) - \left(\lambda_2 s_1 s_2 + \frac{k_2}{N}s_1\right) \quad (12)$$

$$\frac{ds_2}{dt} = \left(\mathrm{w}\lambda_2 s_2 + \frac{k_2}{N}\mathrm{w}\right) - \left(\lambda_1 s_1 s_2 + \frac{k_1}{N}s_2\right) \quad (13)$$

$$\frac{dw}{dt} = \left(\lambda_2 s_1 s_2 + \frac{k_2}{N}s_1\right) + \left(\lambda_1 s_1 s_2 + \frac{k_1}{N}s_2\right) -$$

$$\left(\mathrm{w}\lambda_1 s_1 + \frac{k_1}{N}\mathrm{w}\right) - \left(w\lambda_2 s_2 + \frac{k_2}{N}w\right) \tag{14}$$

According to this public opinion model, we use Information Reliability, Personal Reliability and Repetition to further classify the crowd. Because information A and B are opposite to each other, the relationship between them is established as follows:

Personal reliability I = A information reliability * A repetition - B information reliability * B repetition

Where I is a positive value is the trustor of information A, otherwise a negative value is the trustor of information B, and the absolute value of the value is the personal reliability.

Suppose $P_A = P_B = 1$, people who believe in A can be divided into three categories according to the reliability: A_1, A_2 and A_3, which represent the acceptance of information A for 1, 2 and 3 times respectively, their reliability to information A is 1, 2 and 3. The relationship transformation diagram is as follows:

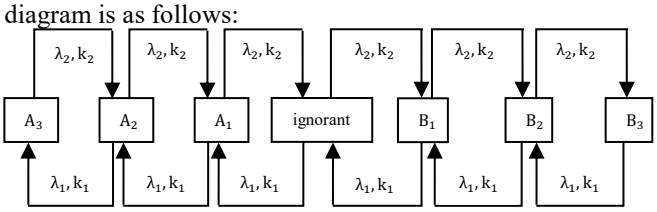


Fig.5 The relationship transformation of different PR

If the model is extended to a more practical situation, the information reliability of A and B will be different, suppose $\mathrm{P}_A = \mathrm{s}, \mathrm{P}_B = \mathrm{t}$, we can assume that $\mathrm{s} > \mathrm{t}$. so that, the diagram of the transformation between groups is shown:

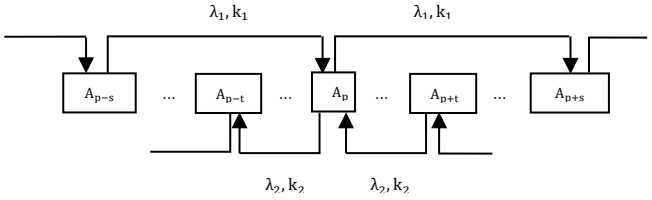


Fig. 6 The transformation of different PR in real world

The proportion of the total number of people whose personal reliability is p is A_P. The equation is shown in the figure above. Among them, $(\sum_{P=1}^{+\infty} A_p)N$ is the number of people who transmit information A, $\lambda_1 \mathrm{A}_{p-s}$ is the number of people who change class A_{p-s} into class A_p per person per day, $k_1 A_{p-s}$ is the number of class A_{p-s} people who are affected by media A to become A_p, and $\lambda_1\left(\sum_{p=1}^{+\infty} A_p\right)NA_{p-s} + k_1 A_{p-s}$ is the number of class A_{p-s} people who become class A_p under the influence of A information. Considering the joint role of media and individuals, $\lambda_1\left(\sum_{p=1}^{+\infty} A_p\right)NA_{p-s} + k_1 A_{p-s}$ is the number of class A_p people increased in unit time. The rest are the same. We can know the number of class A_p people:

$$\begin{aligned}\mathrm{N}\frac{\mathrm{dA_p}}{\mathrm{dt}} = &\left[\lambda_1\left(\sum_{p=1}^{+\infty} A_p\right)NA_{p-s} + k_1 A_{p-s} + \right.\\ &\left.\lambda_2\left(\sum_{p=-1}^{-\infty} A_p\right)NA_{p+t} + k_2 A_{p+t}\right] - \\ &\begin{bmatrix}\lambda_1\left(\sum_{p=1}^{+\infty} A_p\right)NA_p \\ +\lambda_2\left(\sum_{p=-1}^{-\infty} A_p\right)NA_p + (k_1+k_1)A_p\end{bmatrix}\end{aligned} \tag{15}$$

So we can get the total number of groups who receive the information A:

$$\begin{aligned}\mathrm{N}\frac{\sum_{p=1}^{+\infty} dA_p}{\mathrm{dt}} = &\left[\lambda_1\left(\sum_{p=1}^{+\infty} A_p\right)N\left(\sum_{p=1}^{+\infty} A_{p-s}\right) + \right.\\ &k_1\left(\sum_{p=1}^{+\infty} A_{p-s}\right) + \lambda_2\left(\sum_{p=-1}^{-\infty} A_p\right)\left(\sum_{p=-1}^{-\infty} A_p\right)N + \\ &\left.k_2\left(\sum_{p=1}^{+\infty} A_{p+t}\right)\right] - \left[\left[\lambda_1\left(\sum_{p=1}^{+\infty} A_p\right) + \right.\right.\\ &\left.\left.\lambda_2\left(\sum_{p=-1}^{-\infty} A_p\right)\right]N\left(\sum_{p=1}^{+\infty} A_p\right) + (k_1+k_1)\left(\sum_{p=1}^{+\infty} A_p\right)\right]\end{aligned} \tag{16}$$

By changing the parameters to observe the function changes, the simulation effect is achieved. We have:

Side A: $P_a = 6$, $K_a = 1000$, $\lambda\mathrm{a} = 30$;

Side B: $P_b = 5$, $K_b = 800$, $\lambda\mathrm{b} = 25$.

From the above assumptions, we can use MATALB to get the graph (horizontal axis is time, vertical axis is rate. Blue line is proportion of the total number of supporters of A, green line is B):

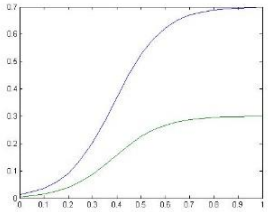


Fig.7 Initial parameter

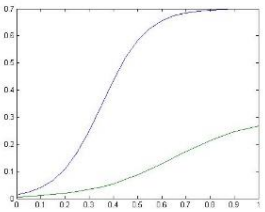


Fig.8 Pa=8

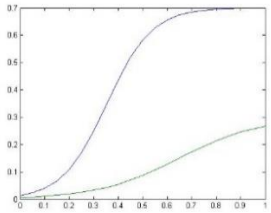


Fig. 9 Ka=1200

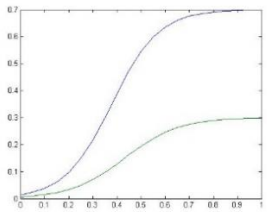


Fig.10 $\lambda\mathrm{a} = 40$

The following conclusions can be drawn:

1. Information Reliability: In the confrontation condition, improving Information Reliability not only

enhances the theoretical supporters of us, but also suppresses the supporters of enemy theories.

2. Media dissemination K：Advance the fastest time for supporters to increase, but for the later stage, the personal dissemination and media influence the growth of the number of supporters together.

3. Personal dissemination λ：Its early stage is limited, but it will play a certain role when the number of theoretical supporters reaches a certain number.

3. Conclusions

Public opinion dissemination is related to people's life and social stability. In this paper, through the analysis of different information and the confrontation condition, the mathematical model of dissemination is constructed. Through numerical simulation and model analysis, we analyze the influence of relevant parameters, and prove some theoretical support for the government's decision making in public opinion control.

References

[1] Boquan Ding, “On the network opinion”, Journalism Review, pp. 4–8, March. 2010.

[2] Wei Cui, Runxi Zeng, Guohua Wang, “Bibliometric analysis of internet public opinion in China”, Information Science, Vol 29, No.1, pp. 131–135, 2011.

[3] Chen Bo, Ling Yu, Junting Liu and Weimin Chu, “Dissemination and control model of internet public opinion in the ubiquitous media environments”, Systems Engineering—Theory & Practice, Vol 31, No. 11, pp. 2140-2150, November. 2011.

[4] Sehulze C, “Sznajd opinion dynamics with global and local neighbourhood”, Int J Mod Phys C, Vol 15, No.6, pp. 867–872, 2004.

[5] Wei Fang, LiuJin He, Kai Sun, et al, “Study on dissemination model of network public sentiment based on cellular automata”, Journal of Computer Applications, Vol 30, No. 3, pp. 751–755, March 2010.

[6] Sznajd W K, Sznajd J, “Opinion evolution in closed community”, Int J Mod Phys C, Vol 11, No.6, pp.1157–1165, 2000.

[7] Changyu Liu, Xiaofeng Hu, Guangya Si, et al, “Public opinion propagation model based on small world networks”, Journal of System Simulation, Vol 18, NO. 12, pp. 3608–3610, December 2006.

[8] Newman M E J, Watts D J, “Scaling and percolation in the small world network model”, Phys Rev E, No. 60, pp. 7332–7342, 1999.

[9] Shiyao Jin, Hongbing Huang, Gaojun Fan, “Emergence-oriented research on multi-agent systems and its state of arts”, Chinese Journal of Computers, Vol 3l, No. 6, pp. 881–895, 2008.

[10] Qiyuan Jiang, Jinxing Xie, and Jun Ye. Mathematical model, Higher Education Press, Beijing, 2011.

[11] Sudbury A J, “The proportion of the population never hearing a rumour”, J Appl Prob, NO. 22, pp. 443–446,1985.

[12] Leskovec J, McGlohon M, Faloutsos C, et al, “Patterns of cascading behavior in large blog graphs”, Proc of the SIAM Int Conf on Data Mining, New York, pp. 551–556, 2007.

[13] Gruhl D, Guha R, Liben-Nowell D, et al, “Information diffusion through blogspace”, Proc of the 13th Int Confon World Wide Web, New York, pp. 491–501, 2004.

[14] Yuexin Lan, “Research on Network Rumor Diffusion Model and Countermeasures in the Emergercy”, Information Science, Vol 39, No. 9, pp. 1334-1338, September. 2012.

[15] Zhang Lifan, Zhao Kai, “Study on the Internet Public Opinion Dissemination Model with Discussion Under the Effect of Media”, New Technology of Library and Information Service, Vol 264, No. 11, pp. 60-67, 2015.

Author Index

ZHANG JIE	#03_08	420
ZHANG LINGYI	#02_12	380
ZHANG PING	#02_12	380
ZHANG QUANLIN	#03_12	437
ZHANG SHIBIN	#01_37	166
ZHANG SHIBIN	#01_54	255
ZHANG SHUO	#01_04	14
ZHANG XIAOSONG	#01_51	240
ZHANG XIAOXIAO	#03_12	437
ZHANG XIYI	#01_30	134
ZHAO JUN	#01_46	209
ZHAO JUN	#01_57	271
ZHAO YALING	#01_60	291
ZHENG YAO	#01_47	216
ZHI-GANG MA	#01_11	50
ZHI-GANG MA	#01_12	54
ZHIGANG MA	#01_40	179
ZHIGUANG QIN	#01_15	67
ZHIZHAO FENG	#01_34	153
ZHOU HONGTAO	#01_10	44
ZHOU HUANG	#01_31	138
ZHOU HUANG	#02_09	361
ZHOU JIE	#01_51	240
ZHOU XIAOXUE	#03_05	404
ZHOU YING	#02_12	380
ZHU WENQUAN	#01_06	23
ZHUO YONGNING	#03_05	404
ZILI YOU	#01_19	89
ZOU QIANYIN	#01_63	306
ZOU QIANYING	#01_48	222
ZOU ZONGZHENG	#03_05	404