CONFERENCE PROGRAM

Tianjin, China | April 21-23, 2023

2023 8th International Conference on Multimedia and Image Processing

2023 7th International Conference on Cryptography, Security and Privacy

Sponsored by

Hosted by

Supported by

Society Hill Conference & Resort Hotel.

天津社会山国际会议中心酒店

No. 198 Zhijing Road, South Railway Station, Xiqing District, Tianjing, China.

天津市西青区南站知景道 198 号

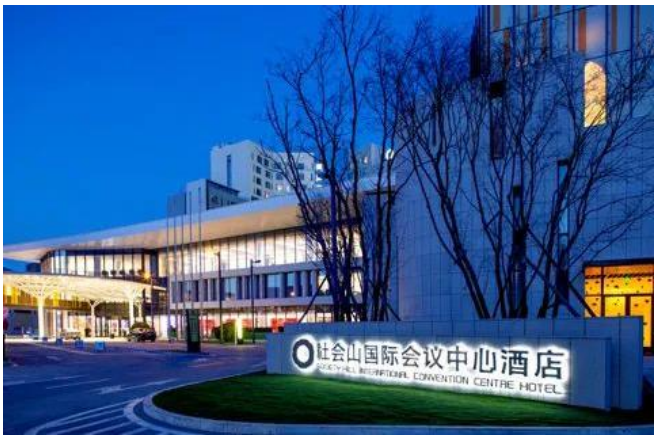
TABLE OF CONTENT

General Information 03
Welcome Message 04
Conference Committee 05
Agenda Overview 07
Introduction of Keynote Speaker 10
On-site Session: Digital Image Analysis and Data Encryption Technology 16
Online Session 1: AI-based Image Analysis and Processing Method 19
Online Session 2: Modern Cryptography Theory and Information Encryption Technology 24
Online Session 3: Information Privacy Protection and Data Security 28
Online Session 4: Cloud Computing and Computer Network 32
Online Session 5: Electronics Engineering 35

Note

GENERAL INFORMATION

A Conference Venue



天津社会山国际会议中心酒店 (Society Hill Conference & Resort Hotel)

天津西青区南站知景道 198 号
No. 198 Zhijing Road, South Railway Station, Xiqing District, Tianjing, China

For room booking/订房请联系: 朱轶 18920631811 (会议团队价)

B Onsite Registration

Registration desk→ Inform the staff of your paper ID→ Sign-in→ Claim your conference kit.

C Devices Provided by the Organizer

Laptops (with MS-Office & Adobe Reader) / Projectors & Screen / Laser Sticks

D Materials Provided by the Presenter

Oral Session: Slides (pptx or pdf version). Format 16:9 is preferred.

Presentations: in English.

E Duration of Each Presentation

Keynote Speech: 45min, including Q&A.

Oral Session: 15min, including Q&A.

F Notice

※ Please wear your delegate badge (name tag) for all the conference activities. Lending your participant card to others is not allowed.

※ Please take good care of your valuables at any time during the conference. The conference organizer does not assume any responsibility for the loss of personal belongings of the participants during conference day.

G Zoom Meeting ID

zoom	Room	Meeting ID	Link
	A	843 8802 8543	https://us02web.zoom.us/j/84388028543
✓ Zoom Download ✓ Zoom Background	B	899 5864 0396	https://us02web.zoom.us/j/89958640396

Note:

1. We recommend that you install the Zoom platform on your computer beforehand. New users can participate in the Zoom meeting **without registration**. (Zoom 新用户可直接输入会议号参会，无需注册账号。)
2. Please set your display name on Zoom before joining the online meeting. For instance,

   Author/Presenter: Paper ID_Name < P0123_Li Lei >

   Listener: Listener_Name < Listener_Li Lei >

WELCOME MESSAGE

We are pleased to welcome you to the joint conference of 2023 8th International Conference on Multimedia and Image Processing (ICMIP) and 2023 7th International Conference on Cryptography, Security and Privacy (CSP). The conference is scheduled for April 21-23, 2023, in Tianjin, co-sponsored by Tianjin University of Technology, China, hosted by School of Computer Science and Engineering. It is technically supported by Egyptian Chinese University (ECU), China Aerospace Science and Industry Corporation Limited (CASIC), University of Limerick (UL), Universidade de Évora - Centro Interdisciplinar de História (CIDEHUS), Universiti Malaysia Sarawak (UNIMAS), Wawasan Open University (WOU), and Gebze Technical University (GTU).

The annual international conference is aimed to bring together the researchers, experts, and scholars around the world to exchange their research results and address open issues in related fields. We hope ICMIP x CSP would be able to achieve its objective in providing an effective forum for academician, researchers, and practitioners to advancing knowledge, research, and technology for humanity. It is one of the leading international conferences for presenting novel and fundamental advances in in field of multimedia, image processing, cryptography, security, and privacy.

2023 Tianjin conference will consist of 6 keynote speeches, successively delivered by Prof. Wei-Shi Zheng (Sun Yat-Sen University), Prof. Yao Zhao (Beijing Jiaotong University), Prof. Hai Jin (Huazhong University of Science and Technology, China), Prof. Changsheng Xu (Chinese Academy of Sciences), Prof. Yong Guan (Iowa State University), and Prof. Lei Meng (Shandong University), followed by 5 technical sessions, with topics: digital image analysis and data encryption technology, AI-based image analysis and processing method, modern cryptography theory and information encryption technology, information privacy protection and data security, cloud computing and computer network.

The papers in the proceedings are accepted after being peer-reviewed by conference committee, international reviewers based on the topic and quality. With the keynote speeches, invited speeches, oral sessions, we'll have an exciting program this year, which will allow participants to present and discuss the latest research and industrial developments in these fields.

On behalf of the organizing committee, we would like to deeply express our heartfelt appreciation to all our delegates, keynote speakers, session chairs, as well as all the committee members involved in the technical evaluation of conference papers and in the organization of the conference for their time, effort, and great contributions.

We also wish that this conference will be an unforgettable and wonderful experience for you.

Finally, we wish you a very successful conference! Hope you will enjoy your stay in Tianjin.

Conference Organizing Committee

ICMIP 2023, CSP 2023

Tianjin

CONFERENCE COMMITTEE

Advisory Committee
Hai Jin, Huazhong University of Science and Technology, China

Honorary Chair
Shengyong Chen, Tianjin University of Technology, China (陈胜勇 天津理工大学 教授/副校长)

Conference Chair
Xianbing Wen, Tianjin University of Technology, China (温显斌 天津理工大学计算机科学与工程学院 教授/副院长)

Conference Co-Chairs
Qinghua Hu, Tianjin University, China (胡清华 天津大学人工智能学院 教授/院长)
Shuangbao Wang, Morgan State University, USA

Program Chairs
Fan Shi, Tianjin University of Technology, China (石凡 天津理工大学计算机科学与工程学院 教授/副院长)
Anan Liu, Tianjin University, China (刘安安 天津大学电气自动化与信息工程学院 教授)
Xiaofeng Wang, Xi'an University of Technology, China
Hiroyuki Kudo, University of Tsukuba, Japan
Xiangyang Hao, Information Engineering University, China

Publicity Chairs
Feifei Zhang, Tianjin University of Technology, China
Phoebe Chen, La Trobe University, Australia
Wen-Huang Cheng, National Yang Ming Chiao Tung University, China
Prof. Jian Dong, Tianjin University of Technology and Education, China

Local Organizing Chairs
Lu Yu, Tianjin University of Technology, China
Fan Qi, Tianjin University of Technology, China

Technical Committees *(in no particular order)*
Maozhi Xu, Peking University, China
Xiwen Zhang, Beijing Language and Culture University, China
Jianbin Qiu, Harbin Institute of Technology, China
Carlos Guardado da Silva, University of Lisbon, Portugal
Norwati Mustapha, Universiti Putra Malaysia, Malaysia
Yusuf Sinan Akgul, Gebze Technical University, Turkey
Luís Corujo, University of Lisbon, Portugal
Jorge Sequeira, Lisbon Accounting and Business School Polytechnic University, Portugal
Pavlo Maruschak, Ternopil Ivan Puluj National Technical University, Ukraine
Mohammad Motiur Rahman, Mawlana Bhashani Science and Technology University, Bangladesh
Nagendra Swamy Siddappa Handarakally, University of Mysore, India
Demian Antony D'Mello, Canara Engineering College, India
Tushar H. Jaware, R.C.Patel Institute of Technology, India
Pooja Agarwal, PES University, India
Jin Zhi, St. John's University, USA
She Kun, University of Electronic Science and Technology China, China
Meghana Kshirsagar, University of Limerick, Ireland
Li Xie, Zhejiang University, China

Kuansheng Zou, Jiangsu Normal University, China
Xin Nie, Wuhan Institute of Technology, China
Lili Nurliyana Abdullah, Universiti Putra Malaysia, Malaysia
Martin Butler, Stellenbosch University, South Africa
Yang Liu, Harbin Institute of Technology (Shenzhen), China
Ting Ma, Southwest Petroleum University, China
Wanwan Li, University of South Florida, USA
Gordon Agnew, University of Waterloo, Canada
Eric Sakk, Department of Computer Science, Morgan State University, USA
Jaouhar Fattahi, Laval University, Canada
Cen Wang, KDDI Research Inc., Japan
Rui Chen, Tianjin University, China
Xinfeng Zhang, Yangzhou University, China
Shenshen Luan, China Academy of Space Technology, China
Shixiang Cao, Beijing Institute of Space Mechanics & Electricity, China
Chau Kien Tsong, Universiti Sains Malaysia, Malaysia
Por Fei Ping, Wawasan Open University, Penang, Malaysia
Hamimah Ujir, Universiti Malaysia Sarawak, Malaysia
Thelma Palaoag, University of the Cordilleras, Philippines
Lei Chen, Shandong University, China
Martin Lukac, Nazarbayev University, Kazakhstan
Yaoling Ding, Beijing Institute of Technology, China
Kabalan Chaccour, Antonine University, Lebanon
Priteshkumar Prajapati, Chandubhai S. Patel Institute of Technology, India
Gabriela MOGOS, Xi'an Jiaotong-Liverpool University, China
Xinli Xiong, National University of Defense Technology, China
Goutham Reddy Alavalapati, Fontbonne University, USA
E. Prince Edward, Sri Krishna Polytechnic College, India
Wei Li, Beijing Jinghang Computation and Communication Research Institute, China
Xiaochun Cheng, Middlesex University, UK
Ashraf Darwish, Helwan University, Russia
Paulo Batista, Cultures and Societies of the University of Evora, Portugal
Almas Abbasi, International Islamic University Islamabad, Pakistan
Yanqi Gu, University of California, USA

AGENDA OVERVIEW

FRIDAY, APRIL 21, 2023	
13:30~17:00	On-site Registration (天津社会山国际会议中心酒店 <1F> Society Hill Conference & Resort Hotel)
13:30~17:00	Zoom Test Session (Room A: 843 8802 8543, Link: https://us02web.zoom.us/j/84388028543)

Timetable of Zoom Test Session			
13:30~14:00	14:00~14:30	14:30~15:00	15:00~15:30
P0002	P005	P046	P033
P0006	P013	P047	P044
P0007	P043	P031	P022
P0008	P015	P003	SG507
P0017	P020	P006	SG509
P0018	P032	P023	SG512
P0022	P010	P0003	SG511
P0024	P038	P2001	SG513
P0025	P019	P002	P0005
P0028	P007	P004	/
P0030	P039	P018	/
15:30~17:00	Other online participants, includes but not limited to keynote speaker, session chair, committee member, listener.		

Participants who are going to do an online presentation are required to join the rehearsal in Zoom on Friday, April 21. Duration: 2~3min apiece. Feel free to leave after you finish the test.

线上报告的参会人需参加 4 月 21 号的 Zoom 测试以确保之后的正式发表有序进行。每人大约需要 2~3 分钟，完成即可离开。

AGENDA OVERVIEW

SATURDAY, APRIL 22, 2023

天津社会山国际会议中心酒店 <3F> Society Hill Conference & Resort Hotel

08:00~08:30 On-site Registration *For offline participant who is not able to sign in on the first day.*

Meeting Room 2 <3F> 多功能 2 号厅 | Zoom A: 843 8802 8543

08:30~ Chairperson:
Assoc. Prof. Lu Yu (Local Organizing Chair, Tianjin University of Technology, China)

08:30~08:45 Opening Speech
Prof. Shengyong Chen (Honorary Chair x Tianjin University of Technology, China)
(陈胜勇 天津理工大学 教授/副校长)

08:45~09:30 Keynote I
"Dataflow based High Efficient Graph Processing Accelerator"
Prof. Hai Jin (Huazhong University of Science and Technology, China)

09:30~10:15 Keynote II
"Weakly Supervised & Interactive Image Segmentation"
Prof. Yao Zhao (Beijing Jiaotong University, China)

10:15~10:45 Group Photo / Coffee Break

10:45~11:30 Keynote III
"Connecting Isolated Social Multimedia Big Data"
Prof. Changsheng Xu (Institute of Automation, Chinese Academy of Sciences, China)

11:30~12:15 Keynote IV
"Adaptive Action Assessment Methods"
Prof. Wei-Shi Zheng (Sun Yat-sen University, China)

12:15~13:30 Lunch Buffet (巴里巴里餐厅 Bali Bali <5F>)

13:30~14:10 Keynote V
"RUDBA: Reusable User-Device Biometric Authentication Scheme for Multi-service Systems"
Prof. Yong Guan (Iowa State University, USA)

14:10~14:30 Coffee Break

Meeting Room 2 <3F> 多功能 2 号厅 | **#腾讯会议:** 531-806-128

14:30~17:15 **On-site Session:** Digital Image Analysis and Data Encryption Technology
P021 P042 P024 P0013 P012 P0015 P016 P011 P041 P017 P0023

17:15~19:00 Dinner Time (Room V2 <5F>)

AGENDA OVERVIEW

Room A: 843 8802 8543 || Link: https://us02web.zoom.us/j/84388028543

14:30~17:30 **Online Session 1**: AI -based Image Analysis and Processing Method

P0002 P0006 P0007 P0008 P0017 P0018 P0022 P0024 P0025 P0028 P0030 P0005

Room B: 899 5864 0396 || Link: https://us02web.zoom.us/j/89958640396

14:30~17:45 **Online Session 2**: Modern Cryptography Theory and Information Encryption Technology

P005 P013 P043 P015 P020 P032 P010 P038 P019 P007 P022 P046 P039

SUNDAY, APRIL 23, 2023

Room A: 843 8802 8543 || Link: https://us02web.zoom.us/j/84388028543

09:00~09:40 Keynote VI
"Learning with Multimodal Interactions for Visually-Aware Diet Management"
Prof. Lei Meng (Shandong University, China)

09:40~11:10 **Online Session 4**: Cloud Computing and Computer Network

SG507 SG509 SG512 SG511 SG513 SG505

11:10~11:20 Break time

11:20~12:50 **Online Session 5:** Electronics Engineering

SG514 SG004 SG515 SG005 SG516 SG006

Room B: 899 5864 0396 || Link: https://us02web.zoom.us/j/89958640396

09:40~12:40 **Online Session 3:** Information Privacy Protection and Data Security

P031 P003 P006 P023 P0003 P2001 P002 P004 P018 P033 P044 P047

Note: We will capture a group photo at the end of each online session for the presenters and chairs.

INTRODUCTION OF KEYNOTE SPEAKER

Prof. Hai Jin
Fellow of IEEE, CCF, and Life Member of ACM.

Huazhong University of Science and Technology, China

Dataflow based High Efficient Graph Processing Accelerator

Abstract: With the rapid growth of big data, it is harder and harder to processing these ever-growing data with traditional computer architecture. Dataflow-based architecture provides a new way to tackle above challenge. This talk first briefly introduces the challenges in processing big data and also the difficulties in processing graph computing, then introduce some research results we have done during these years in using dataflow for graph computing. Finally, some future directions for dataflow architecture and also when used in graph computing are introduced.

Hai Jin received the PhD degree in computer engineering from Huazhong University of Science and Technology, in 1994. He is a Cheung Kung scholars chair professor of computer science and engineering with Huazhong University of Science and Technology. In 1996, he was awarded a German Academic Exchange Service fellowship to visit the Technical University of Chemnitz in Germany. He worked with The University of Hong Kong between 1998 and 2000, and as a visiting scholar with the University of Southern California between 1999 and 2000. His research interests include computer architecture, virtualization technology, cluster computing and cloud computing, peer-to-peer computing, network storage, and network security. He was awarded Excellent Youth Award from the National Science Foundation of China in 2001. He is the chief scientist of ChinaGrid, the largest grid computing project in China, and the chief scientists of National 973 Basic Research Program Project of Virtualization Technology of Computing System, and Cloud Security. He has co-authored 22 books and published more than 700 research papers. He is a fellow IEEE, CCF, and a life member of the ACM.

INTRODUCTION OF KEYNOTE SPEAKER

Prof. Yao Zhao
Member of the State Council Discipline Evaluation Group for the discipline of "Information and Communication Engineering"

Beijing Jiaotong University, China

Weakly Supervised & Interactive Image Segmentation

Abstract: Image semantic segmentation is an interdisciplinary research direction involving computer vision, pattern recognition, and artificial intelligence. It is a key scientific issue in applications such as autonomous driving, intelligent monitoring, virtual reality, medical image diagnosis, and robotics. At present, deep learning has made significant breakthroughs in the field of image semantic segmentation. However, a large number of pixel level annotations typically require a significant amount of time, money, and manpower. Therefore, the insufficient or missing training data has become one of the key factors restricting the further development of image semantic segmentation.

In order to reduce the huge burden of pixel level annotation, many weakly supervised image semantic segmentation techniques have been proposed in recent years, which utilize a large amount of easily obtainable weakly supervised information (such as image labels) to complete more complex image semantic segmentation tasks.

Interactive semantic segmentation is an important technical means to reduce the cost of pixel level annotation by guiding computers to achieve fast and accurate object segmentation through simple human-computer interaction.

This report will introduce some research works of my research group in weakly supervised image semantic segmentation and interactive image segmentation.

Prof. Yao Zhao is a distinguished Changjiang Scholar, a Distinguished Young Scholar of NSFC, a leader in scientific and technological innovation of the Ten Thousand Talents Program, IEEE Fellow. He is currently the director of the Institute of Information Science at Beijing Jiaotong University and the director of the Beijing Key Laboratory of Modern Information Science and Network Technology. His research field is digital media information processing and intelligent analysis, including image/video compression, digital media content security, media content analysis and understanding, artificial intelligence, etc. He is leading or led over 30 projects including the 2030 New Generation Artificial Intelligence Project, the 973 Plan, and the 863 Plan for technological innovation. He has published over 200 papers in international journals and conferences, including IEEE Transactions. As the first prize winner, Prof. Zhao has won 5 provincial and ministerial level awards such as the first prize of the Beijing Science and Technology Award. Eight doctoral students under his guidance won the Excellent Doctoral Dissertation Award of Beijing and China Computer Federation. He was invited to serve as an editorial board member for multiple international magazines, including IEEE Transactions on Cybernetics, IEEE Transactions on Circuits and Systems for Video Technology. He is a member of the State Council Discipline Evaluation Group for the discipline of "Information and Communication Engineering" and an expert of the Cloud Computing and Big Data Special Project of the Key R&D Program of the Ministry of Science and Technology.

INTRODUCTION OF KEYNOTE SPEAKER

Prof. Changsheng Xu
ACM Distinguished Scientist, IEEE Fellow, and IAPR Fellow

Connecting Isolated Social Multimedia Big Data, China

Connecting Isolated Social Multimedia Big Data

Abstract: The explosion of social media has led to various Online Social Networking (OSN) services. Today's typical netizens are using a multitude of OSN services. Exploring the user-contributed cross-OSN heterogeneous data is critical to connect between the separated data islands and facilitate value mining from big social multimedia. From the perspective of data fusion, understanding the association among cross-OSN data is fundamental to advanced social media analysis and applications. From the perspective of user modeling, exploiting the available user data on different OSNs contributes to an integrated online user profile and thus improved customized social media services. This talk will introduce a user-centric research paradigm for cross-OSN mining and applications and some pilot works along two basic tasks: (1) From users: cross-OSN association mining and (2) For users: cross-OSN user modeling.

Changsheng Xu, is a distinguished professor of Institute of Automation, Chinese Academy of Sciences. His research interests include multimedia content analysis/indexing/retrieval, pattern recognition and computer vision. He has hold 50 granted/pending patents and published over 300 refereed research papers including 100+ IEEE/ACM Trans. papers in these areas. Prof. Xu is Editor-in-Chief of Multimedia Systems. He serves/served Associate Editor of IEEE Trans. on Multimedia and ACM Trans. on Multimedia Computing, Communications and Applications. He received the Best Paper Awards of ACM Multimedia 2016 and 2016 ACM Trans. on Multimedia Computing, Communications and Applications. He served as Program Chair of ACM Multimedia 2009. He has served as associate editor, guest editor, general chair, program chair, area/track chair, special session organizer, session chair and TPC member for over 20 IEEE and ACM prestigious multimedia journals, conferences and workshops. He is an ACM Distinguished Scientist, IEEE Fellow, and IAPR Fellow.

INTRODUCTION OF KEYNOTE SPEAKER

Prof. Wei-Shi Zheng
Associate Dean of School of Data and Computer Science

Sun Yat-sen University, China

Adaptive Action Assessment Methods

Abstract: Action assessment is to evaluate how well an action is performed, is an important task in human action analysis. Action assessment has experienced considerable development based on visual cues; however, existing methods neglect to adaptively learn different architectures for varied types of actions and are therefore limited in achieving high-performance assessment for each type of action. In fact, every type of action has specific evaluation criteria, and human experts are trained for years to correctly evaluate a single type of action. Therefore, it is difficult for a single assessment architecture to achieve high performance for all types of actions. However, manually designing an assessment architecture for each specific type of action is very difficult and impracticable. In this talk, we will present an adaptive action assessment work, which adaptively designs different assessment architectures for different types of actions. We also further show that such an adaptive idea can also be used to model the interaction between multiple instances during the assessment for different tasks. We will demonstrate the visual interpretability of our model by visualizing the details of the assessment process.

Dr. Wei-Shi Zheng is now a full Professor with Sun Yat-sen University. He has now published more than 130 papers in main journals and top conferences (ICCV, CVPR, IJCAI, AAAI). His research interests are in computer vision and machine learning algorithms, particularly focusing on person/object association and activity understanding, and the related weakly/self-supervised machine learning methods. He received outstanding review awards in recent top conferences (ECCV 2016 & CVPR 2017), and received the outstanding area chair award for ICME 2020. He has been an area chair/senior PCs of CVPR, ICCV, BMVC, IJCAI, and NeurIPS. He has been a technical programme chair of ICME 2022. He is an IEEE MSA TC member and an IEEE VSPC TC member as well. He is an associate editor of IEEE TPAMI and Pattern Recognition. He has also joined Microsoft Research Asia Young Faculty Visiting Programme. He is a recipient of the Excellent Young Scientists Fund of the National Natural Science Foundation of China, and a recipient of the Royal Society-Newton Advanced Fellowship of the United Kingdom.

INTRODUCTION OF KEYNOTE SPEAKER

Prof. Yong Guan
Fellow of American Academy of Forensic Sciences (AAFS)
Iowa State University, USA

RUDBA: Reusable User-Device Biometric Authentication Scheme for Multi-service Systems

Abstract: The essence of information assurance resides in the ability to establish trust relationship among communication parities. The authentication and verification of user and device identities require cost-effective solutions. Two emerging approaches, biometric authentication and devices' fingerprint, allow users and devices to prove their identity efficiently and securely. In real-world applications, users are inclined to register to multiple services with the same secret information. However, the potential risks brought by the reuse of secret information need to be taken seriously. In this talk, we will present the RUDBA scheme, a novel reusable user-device biometric authentication scheme that captures the user's biometrics and the device's fingerprint. The extracted confidential is fused as authentication material for the user-device pair's identity, and can provide a symmetric key for the subsequent communications. This scheme is implemented using the public biometric dataset and the intrinsic SRAM PUF data. We have evaluated the scheme, and the experimental results showed that the RUDBA scheme has the potential to lead to a reliable and reusable users-device authentication system. This line of research starting from our Adopted-Pet protocol and other SRAM PUF based solutions, has created a fruitful set of research opportunities and new paradigms in securing the next-generation wireless networks/applications such as IoT, 5G, and Internet systems

Dr. Yong Guan is a professor of Electrical and Computer Engineering, and Cyber Forensics Coordinator of the NIST Center of Excellence in Forensic Sciences – CSAFE. He received his Ph.D. degree in Computer Science and Engineering from Texas A&M University in 2002, MS and BS degrees in Computer Science from Peking University in 1996 and 1990, respectively. With the support of NSF, IARPA, NIST, ARO, and Boeing, his research focuses on security and privacy issues, including digital forensics, network security, and privacy-enhancing technologies for the Internet. The resulted solutions have addressed issues in mobile app forensic analysis, attack attribution, secure network coding, key management, localization, computer forensics, anonymity, and online frauds detection. He served as the general chair of 2008 IEEE Symposium on Security and Privacy (Oakland 2008, the top conference in security), co-organizer for ARO Workshop on Digital Forensics, and the co-coordinator of Digital Forensics Working Group at NSA/DHS CAE Principals Meetings. Dr. Guan has been recognized by awards including NSF Career Award, ISU Award for Early Achievement in Research, the Litton Industries Professorship, and the Outstanding Community Service Award of IEEE Technical Committee on Security and Privacy. Dr. Guan serves as a Board member of Trusted Computing Center of Excellence (TCCoE), and is a Fellow of American Academy of Forensic Sciences (AAFS).

INTRODUCTION OF KEYNOTE SPEAKER

Prof. Lei Meng
Associate Editor of Applied Soft Computing, PC member of top-tier conferences, such as MM, AAAI, IJCAI, and SIGIR.
Shandong University, China

Learning with Multimodal Interactions for Visually-Aware Diet Management

Abstract: Visual food logging, usually embedded in mobile phone apps, is an emerging tool for diet management. It allows users to upload food photos of their daily intake and provides personalized services to encourage users to retain a healthy eating style. To achieve these, food recognition and recommendation are two key functionalities. However, the performance of learning to recognize food content, such as food name and its ingredients, from images is usually limited by the diverse appearances of images. This also makes modeling users' eating preferences based on these images more difficult. This talk presents our recent achievements on learning representations of food images for improved recognition and recommendation. Both are achieved by leveraging another view of food, i.e. the tagged ingredients, to regularize the encoding of image features. In food recognition, the multimodal assumption allows the use of transfer learning to map the representations of images to those of ingredients, thus taking advantage of their stronger discriminative power. Food recommendation is more challenging since users typically eat food in different categories, requiring the image features to go beyond semantics, referred to as collaborative similarity. We will show how to encode both the semantic and collaborative similarities in image representation via a continual multitask learning approach. Besides the technical details, backgrounds, key challenges, and the experimental findings will be discussed.

Lei Meng is Professor with the School of Software, Shandong University. He received the B.Eng.'s degree in 2010 from Shandong University, China, and obtained the PhD's degree in 2015 from Nanyang Technological University. From 2015 to 2020, he worked successively at Nanyang Technological University and National University of Singapore as Research Fellow and Senior Research Fellow. His research interests include multimedia computing, deep learning, and its applications in healthcare and digital twin for social governance. He has published a book with Springer and fifty conference and journal papers at top and renowned venues, such as MM, AAAI, TKDE and TNNLS. He serves as the Associate Editor of Applied Soft Computing, and the (senior) program committee member of top-tier conferences, such as MM, AAAI, IJCAI, and SIGIR.

ON-SITE SESSION

SATURDAY, APRIL 22, 2023
On-site Session: Digital Image Analysis and Data Encryption Technology
Chairperson: TBA

Meeting Room 2 <3F>
多功能 2 号厅
#腾讯会议：531-806-128

14:30-14:45 P021	Detection of conflicts between APP's Privacy Policy and Actual Behavior: A Security Analysis System Yang Liu, Harbin Institute of Technology, Shenzhen, China Abstract-Leaks of user privacy in the mobile cloud environment have been common in recent years. Common APP stores require apps to have a user privacy policy that complies with applicable laws. Due to the problem of lengthy papers or difficultto-understand sentences in privacy policies, users frequently skip reading them or fail to comprehend them. Moreover, there may be conflicts between the privacy policy and the actual behaviors. In order to alleviate these problems above, we design a security analysis system that employs natural language processing to detect conflicts between an APP's privacy policy and its actual behaviors. Experimental results show that the analysis accuracy is improved compared with existing methods.
14:45~15:00 P042	A Related Key Attack on the Word-Oriented BeepBeep Stream Cipher Zhiyi Liao, PLA SSF Information Engineering University, China Abstract-The word-oriented BeepBeep stream cipher, developed by Driscoll in FSE 2002, is proposed to provide secrecy and integrity for embedded real-time systems. There has been no attack on the stream cipher published so far. By exploiting a weakness of the BeepBeep stream cipher during its initialization, this paper proposes a key recovery attack on the BeepBeep stream cipher in the related key setting. The attack recovers the 192-bit secret key of BeepBeep with a time complexity of 2128, requiring two related keys, 232 chosen IVs and 233 keystream words. This is the first cryptanalytic attack on BeepBeep which is significantly better than an exhaustive key search. The result shows that the BeepBeep stream cipher is vulnerable against the related key attack and can not provide 192-bit security.
15:00~15:15 P024	Mission-oriented Security Framework: an Approach to Embrace Cyber Resilience in Design and Action Xinli Xiong, National University of Defense Technology, China Abstract-The rapid development in IT and OT system makes interactions among themselves and with humans immerse in the information flows from the physical to cyberspace. The traditional view of cyber-security faces challenges of deliberate cyber-attacks and unpredictable failures. Hence, cyber resilience is a fundamental property that protects critical missions. In this paper, we presented a mission-oriented security framework to establish and enhance cyber-resilience in design and action. The definition of mission-oriented security is given to extend CIA metrics of cyber-security, and the process of mission executions is analyzed to distinguish the critical factors of cyber-resilience. The cascading failures in inter-domain networks and false data injection in the cyberphysical system are analyzed in the case study to demonstrate how the mission-oriented security framework can enhance cyber resilience.
15:15~15:30 P0013	Single-station multi-view global calibration based on the concentric circle 3D target Pengfei Sun, Beihang University, China Abstract-In view of the disadvantage that traditional tracking 3D scanners can only use global binocular camera to complete single-station multi-view global calibration, a concentric circle 3D target (CC3DT) is designed in this paper. For the designed CC3DT, a single-station multi-view global calibration algorithm is proposed. This method only needs one camera to complete the global calibration function of global binocular camera. The designed CC3DT has simple structure and low cost. In this paper, the validity and feasibility of the proposed global calibration algorithm are verified by real experiments. It has widely application prospect and practical theoretical research value.

15:30~15:45 P012	Verifiable Threshold Multiplication Protocol based on Oblivious Transfer Sam Ng, Crypto.com, Hong Kong Abstract-Shamir Secrets Sharing (SSS) is one of the foundations of many Multi-Party Computation (MPC) protocols. While SSS can handle linear combinations of multiple secrets natively, handling the multiplication of secrets increases its "degree" and therefore require more participants in general. In this paper, we present a verifiable method to handle the multiplication of SSS without increasing the degree. Our method is based on the Gilboa Protocol or its variants, which itself is built on top of Oblivious Transfer (OT). We sketch a security analysis that the method is secure under a malicious adversary security model. And as an application use case, we show a new ECDSA threshold signature scheme built on top of our method.
15:45~16:00 P0015	Arbitrary Style Transfer with Multiple Self-Attention Yu Song, Shandong Normal University, China Abstract-Style transfer aims to transfer the style information of a given style image to the other images, but most existing methods cannot transfer the texture details in style images well while maintaining the content structure. This paper proposes a novel arbitrary style transfer network that achieves arbitrary style transfer with more local style details through the cross-attention mechanism in visual transforms. The network uses a pre-trained VGG network to extract content and style features. The self-attention-based content and style enhancement module is utilized to enhance content and style feature representation. The transformer-based style cross-attention module is utilized to learn the relationship between content features and style features to transfer appropriate styles at each position of the content feature map and achieve style transfer with local details. Extensive experiments show that the proposed arbitrary style transfer network can generate high-quality stylized images with better visual quality.
16:00~16:15 P016	A New Research on Verifiable and Searchable Encryption Scheme Based on Blockchain Zhong Kang, Central University of Finance and Economics, China Abstract-Cloud storage attracts more and more individuals and enterprises to outsource and store data on cloud servers due to its advantages of high efficiency, speed, low economic cost and on-demand access. Due to privacy requirements, data files need to be uploaded after being encrypted. Current searchable encryption technology enables retrieval of encrypted data, but lacks verification of searched results. In response to the above problem, this paper proposes a new searchable encryption scheme based on blockchain, which supports multi-keyword ranked search together with verification of searched results. Concretely, the scheme first encrypts the data and uploads it to the cloud server, then builds the index via blockchain. By calling the smart contracts to execute the search algorithm, the search result is returned to the user and the hash value is verified, which ensures the integrity and accuracy of the searched result. Secondly, by combining the vector space model and BM25 model to construct the index and query of encrypted data, the ranked search for multiple keywords is realized, in which the keyword balanced binary tree index is established to improve the retrieval efficiency. Experimental results show that the improved scheme has higher search accuracy while ensuring retrieval efficiency.
16:15~16:30 P011	Classification and application of long-duration flows based on flow behavior Zihao Chen, School of Cyber Science and Engineering, Southeast University, China Abstract-Long-duration flows are extended network flows in the Internet that result from various network activities such as file transfers, persistent connections, and control command transmissions. These flows are utilized by a broad range of applications in the Internet, both benign and malicious, and their management and security are crucial for the functioning of the Internet. In this study, we categorize long-duration flows into three types: control flows, mixed flows, and information flows, based on their purpose for existence. Subsequently, features are extracted based on three characteristics: flow, time series, and packet length. The selected features are used to construct a dataset for training a classification model. The empirical analysis of real-world traffic data from high-speed network boundaries demonstrates that the classification model is capable of accurately identifying control flows in long-duration flows and determining specific applications within them.

16:30~16:45 P041	A Survey on Cross-chain Data Transfer Wei Zheng, Hainan University, China Abstract-Blockchain technology is moving towards multichain interconnection, i.e., various blockchains sharing data, assets and functions to collaborate. To enable different blockchains to work together, Cross-chain Data Transfer technology is significant and developing rapidly, attracting the attention of both industry and academia. This paper defines Cross-chain Data Transfer (CDT) at the level of technical goals, explains the unique importance of CDT and discuss schemes for designing CDT approaches. We collect the latest approaches that have been applied in the field and analyze their advantages and disadvantages. Moreover, we discuss future challenges and research directions, show the broad research prospects in the field of CDT technology.
16:45~17:00 P017	Cryptomining Traffic Detection Based on BiGRU and Attention Mechanism Yijie Huang, School of Cyber Science and Engineering, Southeast University, China Abstract-The increasing popularity of cryptocurrencies has led to a rise in cryptomining attacks, where attackers unauthorizedly use the victim's computer resources to mine digital currency. This brings significant financial losses and security risks to both personal and professional life. Therefore, the detection of cryptomining attacks is of paramount importance. The conventional packet inspection technique is no longer effective due to the use of encryption. Moreover, the prevalent machine learning methods rely heavily on features extracted by professional experience, which is time-consuming. In this paper, we analyze the features of real-world campus cryptomining traffic and propose an end-to-end deep learning model for malicious mining detection. Our model, based on Bidirectional Gate Recurrent Unit (BiGRU) with an attention mechanism, extracts representative features from the raw flow. The results indicate that our approach outperforms benchmark models and previous methods on the large-scale imbalanced dataset, achieving a G-mean value of 0.99 with only 8 packets of a flow.
17:00~17:15 P0023	MFC-Net: A Multiple Feature Complementation Network for Person Re-identification in Aerial Imagery Zichen Yin, Shandong Normal University, China Abstract-Person re-identification on Unmanned Aerial Vehicles (UAVs) platforms has received widespread attention, but visual monitoring on UAVs is affected by pixels, angles, and more misalignment, which impairs the discriminative ability of the learning representation and brings new challenges to person re-identification tasks. In order to solve the problem, we propose a Multiple Feature Complementation Network (MFC-Net). MFC-Net consists of two modules, the Parallel Dual Attention Modules (PDAM) and the Multilayer Feature Fusion Module (MFFM). The PDAM consists of two attention branches—Multiscale Channel Attention (MCA) and Weighted Positional Attention (WPA). The PDAM can effectively perceive regional features and better focus the image. The MFFM further fuses two complementary attention features, which effectively solves the problems of angle and misalignment and improves the accuracy of person re-identification. Compared with existing techniques, MFC-Net performs well in the person re-identification of aerial imagery.

ONLINE SESSION 1

SATURDAY, APRIL 22, 2023 Room A: 843 8802 8543

Online Session 1: AI-based Image Analysis and Processing Method

Chairperson: TBA

14:30~14:45 P0002	UPerNet-Based Deep Learning Method for the Segmentation of Gastrointestinal Tract Images Yang Qiu, University of Wisconsin-Madison, USA Abstract-When giving radiation therapy to patients with gastrointestinal cancers, radiation oncologists must manually outline the locations of the stomach and intestines in order to adjust the direction of the X-ray beam. This process can increase the dose delivered to the tumor while avoiding the stomach and intestines, but is time-consuming and labor-intensive. Therefore, the development of automated segmentation methods for gastrointestinal tract images will enable faster and more effective treatment for patients. For that purpose, we propose an UPerNet-based deep learning approach in this paper, to segment the stomach, small bowel, and large bowel in gastrointestinal tract images with excellent performance. The dataset in this work is from the UW-Madison GI Tract Image Segmentation Kaggle competition. The input images are obtained by applying a 2.5D preprocessing method on this dataset. We choose the EfficientNet-B4 and Swin Transformer (base) as the backbones of the UPerNet architecture separately. An average ensemble of these two models is subsequently implemented to boost the model performance. After applying the K-Fold cross validation, our method reaches a competition score 0.86827 on the private test set. With this performance, our team locates at the 135th place among 1548 teams and gets a bronze medal in the Kaggle competition. This work would accelerate the development of auxiliary systems for the segmentation of gastrointestinal tract images, and could potentially contribute to the research of generalized segmentation methods for medical images.
14:45~15:00 P0006	Secure image retrieval based on deep learning in cloud computing Sijie Li, Hunan University, China Abstract-The rapid growth of multimedia data and the limited storage and computing capacity of local devices motivate the outsourcing service of cloud storage. For the outsourced images, users usually encrypt them to protect their privacy and require the ability to retrieve them later. Therefore, how effectively managing and retrieving massive encrypted images in cloud servers becomes a challenging problem. In this paper, we propose a deep learning-based image retrieval scheme for cloud computing. Firstly, we use a Convolutional Neural Network (CNN) to extract feature descriptors and represent each image as two parts: image category and image feature. Then, we construct an encrypted tree-based index structure to improve retrieval efficiency. At the same time, we use the Learning With Errors (LWE)-based secure k-Nearest Neighbor (kNN) algorithm and random matrix to protect the security of two parts of the descriptors. The feasibility of our scheme is proved through security analysis. Finally, we conduct empirical experiments on the Caltech256 image dataset, and the results show that our scheme can achieve high retrieval efficiency and accuracy while ensuring image security.
15:00~15:15 P0007	Multimodal Emotion Detection based on Visual and Thermal Source Fusion Peixin Tian, University of Technology and Science of China, China Abstract-The contactless emotion detection is an interesting research topic today. In this paper, we first study the physiological basis of human emotions to better understand what happens in our body when emotions arise and change. We then introduce the interconnection between the brain trunk vessels and the facial vessels. The investigation reveals that the variations of human emotions could be reflected by facial blood horizontal flow, and the detection of facial blood horizontal flow could be realized by mainly measuring the Remote photoplethysmography (rPPG) and gray scale variation on human cheeks. To validate these findings, we set up an emotional evoking experiment to capture the RGB and thermal videos of human testees, extract out horizontal facial blood flows, and finally classify these features into three different emotions (i.e., fear, happiness and sadness) by learning. The reported classification accuracy reaches 0.841, based on total 45 testees.

15:15~15:30 P0008	Comparative Study of Different Ground Objects Classification Based on UAV Orthophoto Xie Shiqin, China Software Test Center, Beijing, China Abstract-UAV technology is characterized by strong environmental adaptability, flexibility, low cost and high resolution, and has been gradually applied in the field of land use classification in recent years. In order to explore a fast ground objects feature extraction method suitable for high resolution UAV orthophoto image, three commonly used supervised classification methods (Maximum likelihood classification, Mahalanobis distance classification, and Minimum distance classification) are selected to compare and analyze the ground objects feature classification in the study area. The results show that the maximum likelihood classification method is better than the other two classification methods, the classification results are basically consistent with the actual situation, and the overall classification accuracy is 94.21%,1.93% and 11.61% higher than the other two methods respectively; Kappa coefficient can reach 88.29%, which is 4.32% and 14.59% higher than other three methods respectively. Therefore, when the supervised classification method is selected for UAV orthophoto classification, the maximum likelihood method performs best among the three ground objects feature classification methods, and can be given priority in the application of high-resolution UAV orthophoto classification.
15:30~15:45 P0017	Recognition and Detection of UAV Based on Transfer Learning Zhao Ping Hao, Taishan University, China Abstract-With the increasing application scenarios of UAVs in industry, agriculture, military and other fields, the potential threats to national security and public security cannot be ignored. In addition, effective UAV detection and/or tracking is becoming an increasingly important security service. This paper integrates deep learning and image processing technology to conduct research in this context. In this paper, a transfer learning based UAV detection model (YOLOV5-UAV) is proposed. In order to reduce the influence of the amount of supervised data and the imbalance of target distribution on the performance of the model, the dataset is constructed based on self-shot videos and Internet downloaded videos in different natural scenes, combined with Mosaic data enhancement and adaptive scaling techniques. Therefore, the problem of data security is also effectively solved. Furthermore, real-time tests were carried out in two different time periods, namely day and night, from multiple scales, multiple perspectives and multiple natural scenes, for purpose of verifying the validity of the model. The applicability of different detection models is compared and analyzed for small target, moving background and weak contrast between UAV and background. The results show that YOLOV5-UAV model has a good performance in both detection accuracy and detection speed.
15:45~16:00 P0018	Detail-Preserving Video-based Virtual Try-on (DPV-VTON) Jahnavi A B, PES University, India Abstract-Virtual Try-on systems enable the try-on of a desired clothing on a target person image. These systems have led to vast research and have attracted commercial interest. However, the existing techniques are image-based systems limited to using an in-shop target clothing from a pre-defined dataset. To address this, we propose a video-based virtual try-on network DPV-VTON, that simulates the try-on using the target cloth extracted from the fashion videos on a target person image, while preserving the details and the characteristics. The core of the DPV-VTON pipeline is made up of (i) Best Frame Selection (BFS) module that extracts the best frame from the video (ii) Clothing Extraction module (CEM) extracts the target clothing from the selected best frame and generates a binary mask. (iii) A virtual try-on module synthesizes a final virtual try-on. Experiments on the existing benchmark datasets and a curated video dataset demonstrate that DPV-VTON generates photo-realistic and visually promising results. The proposed model obtains the lowest FID, LPIPS and the highest SSIM scores compared to the existing systems.

16:00~16:15 P0022	Design and Implementation of Medical Ultrasound Image Processing System based on MATLAB GUI Shiyan Zheng, Harbin University of Science and Technology, China Abstract-Due to the physical characteristics of ultrasonic imaging, there are many factors in the process of imaging, which lead to the low quality of imaging images. There may be artifacts, noise interference, unclear edge contour of diseased tissue, and other problems. This paper designs and implements an image processing system for medical ultrasound images based on MATLAB GUI. The system realizes the functions of image enhancement, image segmentation, image filtering, edge detection, and morphological processing of medical ultrasound images. Through the detection of breast duct ultrasound images, the noise interference is greatly reduced in the processed ultrasound images compared with the original images. In addition, there is an obvious highlighting effect on the ultrasound images of some typical lesions, which makes the detailed information of the images more obvious and the boundaries of the lesions clearer. The processed images were compared with the original images by subjective evaluation. The evaluation results of professional doctors all show that the treatment method in this paper can greatly improve the readability of medical ultrasound images.
16:15~16:30 P0024	Study of intracranial haematoma localisation based on improved RetinaNet Junyuan Cheng, Changchun University of Science and Technology, China Abstract-Intracranial haemorrhage is described as bleeding within the skull. It is a serious cranio-cerebral disorder recognized for its high mortality and lethality rate, which usually requires urgent follow-up diagnosis and determination of the location and subtype of intracranial hemorrhagic lesions. In this study, we experimented with multiple available deep learning architectures to localize the location of hemorrhagic lesions after traumatic brain injury (ICH). To improve the probability of successful patient resuscitation. In this paper, we propose an improved model based on RetinaNet. The accuracy problem of lesion localisation is not effectively addressed due to the complex structure of the lesion location in intracranial haemorrhage and the large variation in the morphology of the lesion for different subtypes. To address these problems, the paper then proceeds to optimise the original RetinaNet model in terms of its feature extraction network structure, training techniques and Anchor settings. Through comparison experiments, it can be found that the improved model is better than the three target detection models, Faster R-CNN, RetinaNet and YOLOv4.
16:30~16:45 P0025	Reconstruction of hyperspectral images with compressed sensing based on linear mixing model and affinity propagation Youli Zou, Jiangxi University of Science and Technology, China Abstract-The increasing spatial and spectral resolution of hyperspectral images results in a significant rise in data volume, which poses a challenge for data storage and transmission. Therefore, improving the efficiency of storage and transmission by enhancing the reconstruction performance of hyperspectral images at low sampling rates or same sampling rates conditions is a crucial topic in compressed sensing. Previous research has shown that a linear mixing model and distributed compressed sensing method outperform traditional compressed sensing reconstruction algorithms in recovering original data. However, the low estimating accuracy of both the endmembers matrix and abundance matrix due to the random selection of reference bands limits the reconstruction performance. To address this problem, we proposed a compressed sensing reconstruction algorithm based on a linear mixing model and affinity propagation clustering algorithm. Our method improves reconstruction performance by enhancing the estimating accuracy of the endmembers and abundance matrices. During the sampling stage, the affinity propagation clustering algorithm is used to group the spectral bands according to the spectral correlation of hyperspectral images, where the clustering center serving as the reference band and the other bands as non-reference bands. During the reconstruction stage, the number of endmembers from the reference band is estimated fist, and the endmembers matrix and the abundance matrix are then estimated. Finally, the endmembers matrix and estimated abundance matrix are used for reconstruction. Experimental results show that our proposed algorithm achieves higher performance in reconstructing hyperspectral images than the linear mixing model-based distributed compressed sensing method.

16:45~17:00 P0028	Application of Deep Learning in Lunar Volcanic Demo Identification Chen Sun, Macau University of Science and Technology, Macau, China Abstract-Lunar domes have always been one of the important windows to understand lunar volcanic activity, however traditional identification methods for geological domes are expensive, so this study attempts to establish an automatic identification method for lunar volcanic domes. Given that no previous research in this area has attempted to automate the identification of lunar volcanic domes, our team attempted to automate the process for the first time. To achieve the purpose of this research, the researchers first obtained the dome coordinates from the list of known lunar domes and intercepted the data we needed from the corresponding coordinates on the CCD and DEM moon pictures. Subsequently, the researchers screened the data to find data with more obvious features and used these data to train 9 mainstream image recognition models and compared their accuracy rates to verify the feasibility of this study. Finally, the researchers counted the mAP and AP (IoU=0.5) of the nine models and found that the highest of them could reach 0.64 (mAP) and 0.74 (AP). Therefore, this study can conclude that an automated method for identifying lunar volcanic domes should be feasible.
17:00~17:15 P0030	Fast Recognition of Distributed Fiber Optic Vibration Sensing Signal based on Machine Vision in High-speed Railway Security Nachuan Yang, PLA Strategic Support Force Information Engineering University, China Abstract-Accurate and effective identification of multi-vibration events detected based on the phase-sensitive optical time-domain reflectometer (Φ-OTDR) is an effective method to achieve precise alarm. This study proposes a real-time classification method of Φ-OTDR multi-vibration events based on the combination of convolutional neural network (CNN), bi-directional long short-term memory network (Bi-LSTM) and connectionist temporal classification (CTC), which can quickly and effectively identify the type and number of vibrations contained in the data image when multiple vibration signals are present in a single image, and manual alignment is not required for model training. Noncoherent integration and pulse cancellers are used for raw signal processing to generate spatio-temporal images. CNN is used to extract spatial dimensional features in spatio-temporal images, Bi-LSTM extracts temporal dimensional correlation features, and the hybrid features are automatically aligned with the labels by CTC. A dataset of 8,000 vibration images containing 17,589 abnormal vibration events is collected for model training validation and testing. Experiments show that the recognition model C3B3 trained with this method can achieve 210 FPS and 99.62% F1 score on the test set. The system can achieve the real-time classification of multiple vibration targets at the perimeter of high-speed railways and effectively reduce the false alarm rate of the system.
17:15~17:30 P0005	DEEPS: A novel framework for image quality improvement of X-ray non-destructive testing Jianqiang Mei, Tianjin University of Technology and Education, China Abstract-Imaging quality has always been the most critical issue during the analog to digital development of the X-ray non-destructive testing (NDT). Due to the complicated structure of evaluated objects, it is still difficult for human eyes to clearly distinguish foreground objects from the background within the X-ray NDT image. Mean_x0002_while, noise signals of the radiation imaging equipment also cause several shortcomings, such as blurring of key features. Therefore, without upgrading the hardware of industrial inspection systems, there is a strong demand to improve the quality of X-ray NDT images, particularly on content and edges. In this paper, we proposed a novel framework, termed as dual enhancement effectiveness plus sharpening (DEEPS), for quality improvement of X-ray NDT image. Specifically, an alternative implementation of multi-scale retinex with color restoration (MSRCR) is firstly employed to extract and enhance the essential information of the image. Then the combination of contrast limited adaptive histogram equalization (CLAHE) and gamma mapping is sequentially implemented to enhance the contrast and lighting. The output of our proposed framework is finally derived after an unsharp mask (USM) loop. Qualitative and quantitative comparison against the classic methods with Peak Signal-To-Noise Ratio (PSNR), Entropy and Contrast to Improve Index (CII) demonstrate the effectiveness of our proposed framework that effectively improve image quality while preserve the edge information without introducing artefact. In addition, after parallel optimization, our method can be further utilized for real time applications of X-ray non-destructive testing

	scenarios.

ONLINE SESSION 2

SATURDAY, APRIL 22, 2023 Room B: 899 5864 0396

Online Session 2: Modern Cryptography Theory and Information Encryption Technology

Chairperson: TBA

14:30~14:45 P005	Authenticated Identity-based Encryption Scheme with Equality Test for Cloud-based Social Network Jiaojiao Du, South China Agricultural University, China Abstract-Enabling registered users to match friends with the same interest, location, etc. is the most fundamental service provided by social network. With expanding openness of social network, the amount of data is growing exponentially. Cloud computing is then introduced into social network to mitigate the issue of storing and analyzing a substantial amount of data. How to realize user matching while protecting users' privacy remains a key challenge in cloud-based social network. As a cryptography tool, identity-based encryption with equality test (IBEET) can be used to match users with the same interest, location, etc. without decrypting the corresponding ciphertexts, therefore, it can well meet the key challenge in cloud-based social network. In this article, we propose an authenticated identity-based encryption with equality test (A-IBEET) scheme based on the observation that the cloud server may recover users' private information from the ciphertexts through offline message recovery attack (OMRA). Our scheme provides stronger security guarantee for social network users by resisting against OMRA in single-server setting. It could better protect users' privacy without sacrificing efficiency compared with related works.
14:45~15:00 P013	Two Dimensional SOST Extract Multi-Dimensional Leakage for Side-Channel Analysis on Cryptosystems Zheng Liu, Beijing Institute of Technology, China Abstract-In 2021, Perin et al. proposed a horizontal attack framework against elliptic curve scalar multiplication (ECSM) operation based on the work of Nascimento et al. Their framework consists roughly of three steps. First, they apply k-means on the iteration traces from multiple ECSM executions, then, the results of clustering are used to make a leakage metric trace by using sumof-squared t-values (SOST), based on the leakage metric trace, the points of interest (POI) are selected. Second, they apply k-means on those POIs to get initial labels for the scalar bits, the accuracy of initial labels is only $\mathbf{52\%}$. Third, wrong bits are corrected by using an iterative deep learning framework. Our work focuses on improving the horizontal attack framework by replacing SOST with our proposed two dimensional SOST (2D-SOST) to improve the efficiency of POI selection under unsupervised context. 2DSOST can extract leakage information between dimensions while SOST can only extract information on one dimension which limits its performance. By replacing SOST with 2D-SOST, our method improves the accuracy of clustering algorithm from an average of $\mathbf{58\%}$ to an average of $\mathbf{74\%}$. We also simplified the framework used in original paper and finally recover scalar bits successfully under the configuration where the original paper can not.
15:00~15:15 P043	Hill Cipher Modifications and Dynamic Cryptosystem Design MengZe Hong, University of Nottingham Malaysia, Malaysia Abstract-This paper proposes a highly scalable dynamic cryptosystem, Modified Affine Hill Cipher (AHC-M), which effectively addresses the known vulnerabilities of the classical Hill Cipher and provides an innovative design approach to the development of modern cryptography. By analyzing the existing Hill Cipher variations, the key concepts and design principles, such as non-linear encryption, dynamic key expansion, nonsquare matrix algebra and dynamic cryptosystem are investigated in detail. Building on these concepts, two practical modifications are proposed that can significantly improve computational complexity and enhance security. We also propose a cryptanalysis technique by extending the chosen-plaintext attack, which can be applied to break the Affine Hill Cipher and serves as a motivation towards the proposed cryptosystem. Lastly, these concepts are generalized as the starting point for further research.

15:15~15:30 P015	Computation on Jacobians of Hyperelliptic Curves of Genus 3 Zhili Dong, State Key Laboratory of Imformation Security, Institute of Imformation Engineering, CAS. University of Chinese Academy of Science, China Abstract-In this article, we give an easy method to distinguish different cases of additions on Jacobians of hyperelliptic curves of genus 3. In addition, we give an advanced algorithm for group laws on Jacobian of hyperelliptic curves of genus 3. By this method, our algorithm can handle all kinds of inputs without ecalling a generic algorithm. Our method is mainly based on Harley's algorithm. However, we use linear algebra over finite fields, instead of Chinese Reminder Theorem over function fields. Moreover, we did 2 × 108 experiments in the finite field F261−1, our algorithm runs 0.033% faster than previous works in general addition.
15:30~15:45 P020	AES128 Encrypted Image Classification Martin Lukac, Nazarbayev University, Kazakhstan Abstract-The homomorphic cryptographic operations is an umbrella term for computation performed on encrypted data without explicit decryption. The purpose of these operations is to manipulate encrypted data without having to apply decryption first and therefore minimize the computational overhead, breach of anonymity, privacy and without having to disclose private content. One of the promising prospects of homomorphic cryptography is the data classification using neural networks mounted to the back-planes of computational clouds or IoT sensors. While several approaches already explored the classification of encrypted data on specific ciphers, it is yet not well known how well such tasks can be performed on the state of the art AES encryption which was never designed to be homomorphic. In order to provide some insight on this topic, we investigate three different aspects of the classification of AES encrypted data: endto-end learning, transfer learning and the ability of learning the cipher in the context of classification. We compare the performance of network models trained using transfer learning with end-to-end trained models on encrypted data. We also evaluate the classification of encrypted images using Invertible Neural Network (INN) as a mean to learn and predict the encryption of the data, as well as to determine if the learned AES can be efficiently learned. Finally using INN, we evaluate the learning and memorization extent of the encryption: we perform crossdata validation on different combinations of MNIST datasets such as handwritten digits, fashion images and handwritten letters.
15:45~16:00 P032	An Efficient Public Key Encryption with Set Equality Test Xu Zhang, South China Agricultural University, Guangzhou, China Abstract-Public key encryption with equality test (PKEET) provides a method to test whether any two ciphertexts encrypted by different public keys contain the same message without decryption. In practice, users may need to verify the equality of two ciphertext sets. A trivial solution using typical PKEET scheme is testing two ciphertexts respectively from two sets and repeating multiple times until all ciphertexts are tested. Obviously, the above solution not only takes a lot of time, but also discloses the equality between any two ciphertexts in the two sets. To solve the above problem, we present an efficient public key encryption with set equality test (PKE-SET), which does not use the expensive bilinear pairings. Experimental results show that, compared with other PKEET schemes, our PKE-SET has higher computational efficiency and only our PKE-SET does not disclose the equality between any two ciphertexts.
16:00~16:15 P010	Post-mortem of Mega Hacks - Signifying the need for a systemic enterprise view on Information Security Lars Magnusson & Sarfraz Iqbal, Linnaeus University, Sweden Abstract-Once, system thinking was about singular systems. Today we exist in a far more complex world, with systems interacting with systems, directly or indirectly. Information security, therefore, must involve all systems in the chain. New legal European regulations such as Guidelines for Data Protection Regulation demand that the ICT/IT world must include systems outside the organizational border to be involved and accounted for under enterprise information security umbrella. Recent mega hacks analyzed in this article point to the fact that a systems thinking perspective is needed to create modern governance, risk, and compliance security model framework. This research work puts forth a conceptual model based on Viable System Model

	appropriate for a major global information security restructuring. A motive for VSM is grounded in that it works fine with securing modern laws like GDPR and CCPA in supporting a needed enterprise perspective.
16:15~16:30 P038	An Improved DEFAULT-like Cipher via Dynamic Secret S-boxes Against Differential Fault Attack Linyang Yan, Guilin University of Electronic Technology, China Abstract-DEFAULT block cipher presented at ASIACRYPT 2021 was specially designed against differential fault attack (DFA). However, the security of DEFAULT against Information Combining Differential Fault Attack (IC-DFA) was further checked at EUROCRYPT 2022. It is illustrated that IC-DFA can recover the secret key of DEFAULT with less than 100 faults and negligible computational complexity. In this article, a variant cipher based on linear structure and dynamic secret S-box (called DEFAULT-DS) is proposed. More precisely, DEFAULT-DS introduces 15 secret S-boxes, where the selection of these S-boxes is determined by using the round subkey. Moreover, the experimental results show that DEFAULT-DS achieves better security level and stronger resistance against DFA compared with original DEFAULT. In particular, DEFAULT-DS can resist to both the classical DFA and IC-DFA. Furthermore, the software implementation complexity of DEFAULT-DS is similar as DEFAULT.
16:30~16:45 P019	Secure Search over Multi-key Homomorphically Encrypted Data Buvana Ganesh, University College Cork, Ireland Abstract-Homomorphic Encryption (HE) is a very attractive solution to ensure privacy when outsourcing confidential data to the cloud, as it enables computation on the data without decryption. However HE starts to lose effectiveness when scaled to multiple parties. In this paper, we propose the first multi-key HE search and computation framework. To achieve an efficient setup for multi-party search and compute, we explore the different approaches to multi-key HE and secure search schemes to reduce rounds of communication. We propose a novel framework to search homomorphically encrypted data outsourced to a semihonest server and shared with multiple parties dynamically using proxy re-encryption schemes. Our framework performs search with linear search complexity with just one round of communication between the two parties. The protocol provides multi-hop capabilities that enable further computations on the search results.
16:45~17:00 P007	Design and Implementation of a Data Stream Anonymization Core on FPGA Bilal Moussa, Nanomedicine, Imagery and Therapeutics Lab., University of Technology Belfort-Montbeliard, France Abstract-Data privacy has become the center of attention to many researchers and engineers. With high speed data transmission, data privacy can be at risk. Data stream anonymization is a fairly new and effective technique that is being currently investigated. It aims to protect data from third-party attackers. A user must keep in mind that when applying anonymization on a dataset, there will be a tradeoff between data utility and the risk of data identification. In this paper, we propose various anonymization cores that can be used to hide the sensitive parts of the data. The hardware implementation on FPGA of these cores is also discussed. Each implementation takes into consideration the trade-off between the throughput and the power consumption in addition to the application type and specifications. The first architecture treats a simple application where two anonymization techniques are used (i.e. Perturbation and character masking). The second implementation requires more complex anonymization techniques and extends K-anonymity criteria and L-diversity for more sensitive applications where data identification is crucial. Results are compared with existing work implementations and many improvements are applied in terms of resource utilization and throughput.
17:00~17:15 P022	Protecting UAV-Networks: A Secure Lightweight Authentication and Key Agreement Scheme Hulya Dogan, Swansea University, United Kingdom Abstract-Flexible and convenient unmanned aerial vehicles (UAVs), efficient low-altitude alternatives with complex connectivity, serve exciting applications by expanding the versatility of traditional networks and the integration capacity between air and ground nodes. UAVs network trust secure communication to perform the role objectives, enable and coordinate dispatches. However, more efforts are needed toward security by protecting every entity against malicious

	attacks in the network. One open challenge in the UAV network lies in keeping bad actors out of the network and enabling security features for highly heterogeneous and resource-hungry devices (sensors, nodes, actuators). To handle that, we design a new practical security scheme to authenticate the legitimacy of peer device connectivity that is lightweight and secure for UAVs network. The proposed protocol provides mutual authentication between UAV and base station devices. We present a formal security verification using the ProVerif tool as well as old-fashioned cryptanalysis to show that the scheme facilitates various security credentials, such as confidentiality, data integrity, identity privacy, etc., and is resilient against well-known security attacks that impersonation, replay, and forwarding security attacks. We also compare our protocol's performance evaluation (of test-bed) results with state-of-the-art authentication protocols for UAVs based on computation costs.
17:15~17:30 P046	A Case Study of Internet Banking Security of Banks Operated in Bangladesh S. M. Mizanur Rahman, Bangladesh University of Professionals, Bangladesh Abstract-Now a day, Internet Banking is a popular service for the customer of the Banks. As a convenient way of doing banking more and more customers are registering for the internet banking. The banks also getting benefits of providing services to the customer round the clock without any manual involvement of the banker. As all the services done through an automated process, the security features should be implemented properly to protect the customers for any fraudulent transactions. The system should be available round the clock and transactions should be monitors as well as the systems should also monitored for any abnormal behavior of transactions and the system. The hacker group continuously try to penetrate the system and if become successful, the bank and customer both will bear loss. for banks, if the hackers cannot be protected, the bank may go out of business. This study intends to find out the issues of different internet banking site of Bangladeshi banks and recommend the best practices for the banks to be followed to do banking business securely. This will also secure the economy of the Country as a whole, as the banking system is the key to the Economical system of a country.
17:30~17:45 P039	haydIT: An Encryptor and Decryptor Application Marlon Diloy, National University, Philippines Abstract-Encryption is a method of hiding data so that it cannot be read by anyone who does not know the key. The key is used to lock and unlock data. In a hack-prone society like ours now, this method would prevent unauthorized individuals from understanding your most protected correspondences. Hence, the development of an encryptor and decryptor is necessary. haydIT offers a user-friendly interface using intuitive icons that most of us are familiar with. Users can encrypt data, generate private key that serves as a unique lock of encryption, and send it thru any means to its recipient. Receivers can also use the same system to decrypt the data using the private key that must be manually entered to the system. haydIT prides itself in supporting the conversion of different language scriptures, providing asymmetrical way of data conversion through double encryption of randomly selected characters. It also supports multi- level of encryption and applies parity checking for data integrity. Thus, provides a virtually- pattern-less way of encoding and decoding data. The developers utilized the Spiral Methodology in developing the project. It combines the elements of both design and prototyping-in-stages, in an effort to combine advantages of top- down and bottom-up concepts. The developed PC app was tested by 15 IT Professionals based on several metrics and proved that haydIT is performing efficiently as expected with a grand mean of 4.75 interpreted as Excellent. With haydIT, everyone can guarantee that messages will be understood only by its intended reader.

ONLINE SESSION 3

SUNDAY, APRIL 23, 2023 Room B: 899 5864 0396

Online Session 3: Information Privacy Protection and Data Security

Chairperson: Assoc. Prof. Martin Lukac, Nazarbayev University, Kazakhstan

09:40~09:55 P031	Quantum Key Distribution and Security Studies Jianzhou Mao, Morgan State University, USA Abstract-The current development of quantum computing threatens the security of conventional encryption algorithms such as RSA. In recent years, Quantum Key Distribution (QKD) has introduced to the world of information security a viable method that is anticipated to provide security protection against the threat of quantum computing. In this paper, we investigate the protocols of the QKD system. Next, we focus on an experimental study of quantum key distribution. A physical QKD system is leveraged to assist us in further investigating quantum key distribution processes. In our study, an eavesdropper was evaluated to analyze the impact on the QKD processes. In the experimental study results, the difference in key generation, exchange, and error rates between normal and attack scenarios can be observed.
09:55~10:10 P003	An Application Service for Supporting Security Management In Software-Defined Networks Jun Liu, University of North Dakota, USA Abstract-Network functions in Software-Defined Networks (SDN) have been decoupled into a control plane and a data plane. The control plane has become a new target of network attacks. One type of the attack is to compromise one or more SDN controllers. An important research topic is the development of security protection mechanisms for promptly identifying and excluding the compromised SDN controllers from an SDN system. This paper introduces an application service, called portal service layer, for excluding a compromised SDN controller from an SDN system without changing the configuration of an SDN system. The portal service layer is deployed between the control plane and the data plane in an SDN system and functions as a communication mesh to facilitate the communications between the two planes in an SDN system. The portal service layer is an application service constructed based on service mesh which also consists of a data plane and a control plane. Envoy proxies and Consul agents are adopted to materialize the data plane and the control plane, respectively, of the service mesh. Consul agents provide Envoy proxies with the up-to-date routing paths within the communication mesh. A compromised SDN controller can be excluded from an SDN system by preventing it from appearing in any routing path. Envoy proxies enforce the decision of exclusion by relaying the communications between the two planes in an SDN system according to the up-to-date routing paths within the communication mesh.
10:10~10:25 P006	Generating t-Closed Partitions of Datasets with Multiple Sensitive Attributes Vikas Thammanna Gowda, Wichita State University, USA Abstract-The popular t-closeness privacy model requires the "distance" between the distribution of sensitive attribute values in any given raw dataset and their distribution in each equivalence class created to not exceed some privacy threshold t. While most existing methods for achieving t-closeness handle data with just a single sensitive attribute, datasets with multiple sensitive attributes are very common in the real world. We present a method for generating equivalence classes in the presence of multiple sensitive attributes. The equivalence classes generated by our method satisfy t-closeness for even the smallest t value for which t-closeness is achievable and useful for the given dataset, thereby providing the highest possible amount of privacy. Moreover, by generating classes of approximately the same size, our method leads to low information loss caused by generalization of quasi-identifier attributes. Lastly, while generating classes with minimum information loss is known to be NP-hard, our classes with reasonably low information loss can be generated in just polynomial time.

10:25~10:40 P023	A Personal Privacy Risk Assessment Framework based on Disclosed PII Ningning Wu, Information Science Department, University of Arkansas at Little Rock, AR, USA Abstract-Protecting personal identifiable information (PII) is essential for personal privacy and data protection. The leakage of PII can lead to privacy and safety issues like personal embarrassment, workplace discrimination, and identity theft. Driven by privacy laws and regulations, business is becoming more diligent in privacy protection when handling PII. Individual users, on the other hand, are free to produce and share contents online that might contain sensitive information. This paper proposed a personal privacy risk assessment framework from user's perspective. The risk score would help PII owners assess their privacy risks so that they can be more actively control their information release and protect their privacy.
10:40~10:55 P0003	Overlapping Community Discovery Algorithm Based on Seed Node Importance Selection Chen Liu, Tianjin University of Technology and Education, China Abstract-When mining overlapping communities in complex networks, the LFM algorithm uses a random selection of seed nodes, which leads to unstable quality of generated communities. Therefore, a new seed node selection algorithm is proposed. Firstly, the nodes with a large product of network neutrality and relative distance are ranked. The set of nodes and their neighbors are taken as seed communities in order, and these seed communities are well distributed throughout the network, thus improving the stability of the algorithm. The seed communities are then expanded by the fitness function. Finally, the isolated nodes in the network are calculated and similar communities are merged to obtain high-quality overlapping communities. Experiments on real datasets and the LFR benchmark network dataset can eventually lead to higher-quality community structures.
10:55~11:10 P2001	Research on the Sudden Scientific Public Opinion Theme Map and Science Communication Path Method in the Sina Weibo Fan Ruxue, Hong Kong Baptist University, Hong Kong, China Abstract-This research takes sudden scientific public opinion events as the research object, and constructs a public opinion map using LDA, network analysis, and Sankey diagrams. Through methods such as topic division, latent semantic association, and semantic flow, the influence of key words on topics in scientific public opinion is analyzed. The flowing associated words are associated with the source of propagation, and the evolution of scientific communication paths is displayed using knowledge graph visualization. Optimized strategies are proposed for semantic ambiguity, displacement of intermediate nodes, and key user nodes discovered in scientific communication.
11:10~11:25 P002	NIC fingerprint-based switch access control technology Kaiwen Sheng, Southeast University, China Abstract-Almost all existing access control systems authenticate end users based on their digital characteristics, such as MAC addresses. Since digital features are easily forged, these access control systems cannot secure the network well. In this paper, we propose an access control technology based on Ethernet network interface controller (NIC) fingerprint, a physical characteristic, to achieve identity authentication. At the switch side, the physical layer signals from the terminal NIC are collected, and the fingerprint of the NIC is extracted from the physical layer signals using the least mean square error (LMS) adaptive filter. On the basis of MAC address authentication, the proxy mechanism of Remote Authentication Dial In User Service (RADIUS) protocol is adopted to add the NIC fingerprint in the password field of the RADIUS request message, which enables the authentication server to perform two-factor authentication based on the NIC fingerprint and MAC address. The experimental results showed that the recognition accuracy for 75 NICs is 96.6%. In this paper, an access control system was built using a switch, a signal collector, a proxy server and an authentication server to realize that the terminal user was allowed to access the network only when both the NIC fingerprint and the MAC address were legal, which verified the feasibility of the scheme.

11:25~11:40 P004	Secure Multiparty Computation with Identifiable Abort and Fairness Long Nie, National Pilot School of software, Yunnan University, China Abstract-Dishonest majority considered in the SPDZ (the nickname of the protocol of Damgard et al. from Crypto 2012) protocols implies the impossibility of fairness (which means that corrupted parties can prevent the honest parties from learning output). The corrupted parties can learn the outputs of the honest parties and abort the protocol. Settling for the second best, there are many works focusing on the detection of the cheaters. We construct a SPDZ-like protocol which achieves fairness when at most n=2 parties behave maliciously and supports identifiable abort for dishonest majority. We suggest a sharing stage after the parties finish their computation. The parties share the returns of the computation in this stage. The correctness of the sharing is guaranteed by verifiable secret sharing and homomorphic signature. The honest parties can reconstruct the outputs of the cheaters in the setting of an honest majority. We can't prevent the corrupted parties from learning the outputs and aborting the protocol for dishonest majority. Therefore, the sharing stage does not harm to the honest parties. Instead, we provide the honest parties with the identities of all cheaters in this case.
11:40~11:55 P018	Efficient Privacy-preserving Data Aggregation for Lightweight Secure Model Training in Federated Learning Cong Hu, Information Communication Branch State Grid Anhui Electric Power Co., China Abstract-Federated learning has been widely adopted in every aspect of our daily life to well protect the dataset privacy, since the model parameters are trained locally and aggregated to global one, but the data themselves are not required to be sent to servers as traditional machine learning. In State Grid, different power companies tend to cooperate to train a global model to predict the risk of the grid or the trustworthiness of the customers in the future. The datasets belonging to each power company should be protected against another corporation, sector or other unauthorized entities, since they are closely related to users' privacy. On the other hand, it is widely reported even the local mode parameters can also be exploited to launch several attacks such as membership inference. Most existing work to realize privacy-preserving model aggregation relies on computationally intensive public key homomorphic encryption (HE) such as Paillier's cryptosystem, which loads intolerably high complexity on resource-constrained local users. To address this challenging issue, in this paper, a lightweight privacy-preserving data aggregation scheme is proposed without utilizing public-key homomorphic encryption. First, an efficient privacy-preserving data aggregation protocol PPDA is proposed based on any oneway trapdoor permutation in the multiple user setting. Then, based on PPDA, a lightweight secure model training scheme LSMT in federated learning is designed. Finally, security analysis and extensive simulations show that our proposed PPDA and LSMT well protect the sensitive data of power enterprises from collusion attacks, guarantees the security of aggregated results, and outperforms existing ones in terms of computational and communication overhead.
11:55~12:10 P033	Inference Rules for Determined Decisions in Policy-based ABAC Enforcement Systems Pham Thi Bach Hue, Faculty of Information Technology, University of Science, VNU-HCM Viet Nam National University Ho Chi Minh City, Vietnam Abstract-Attribute-based access control (ABAC) model manages access to resource by policies. Incoming requests must satisfy some policy to be permitted to execute. Polices and requests are based on attributes, which are basic elements for constructing four components of each one, including Subject, Environment, Resource and Action. In XACML standard, for a given request the response can be one of the following values: Permit, Deny, Not Applicable and Indeterminate. The two last values are not decisive, bring no value to the requesters. We focus on the requests received Not Applicable in this article. Modifying the polices individually or rewriting the request by reducing the resource from the original one are solutions of existing studies. We theoretically introduce inference rules, which are applied on the policy set for computing the closure of it to evaluate whether the request is responded with firmed decisions of permit or deny. Our proposals guide the security administrators in building the policy set satisfying the important property called completeness-the ability to be able to give determined responses to all the possible legal requests in the real world. In addition, we find out other necessary properties of the policy set and suggest the algorithm for ensuring some of them.

12:10~12:25 P044	A Multi-Strategy Adversarial Attack Method for Deep Learning Based Malware Detectors Fan Yin, School of Cyber Science and Engineering, Southeast University, China Abstract-Deep learning allows building high-accuracy malware detectors without complicated feature engineering. However, research shows that the deep learning model is vulnerable and can be deceived if attackers add perturbation to input samples to craft adversarial examples deliberately. By altering the pixel values of the images, attackers have been able to generate adversarial examples that can fool state-of-the-art deep learning based image classifiers. However, Windows malware is a structured binary program file. Therefore, arbitrarily altering its contents will often break the program's functionality. In order to solve this problem, a standard but inefficient method is to run the sample in the sandbox to verify whether its functionality is preserved. This paper proposes a multi-strategy adversarial attack method, which can generate malware adversarial examples with functionality-preserving. Our method manipulates the redundant or extended space in the Windows malware binary, so it will not break functionality. Experiments show that our method has a high attack success rate and efficiency.
12:25~12:40 P047	White-Box PRNG: A Secure Pseudo-Random Number Generator under the White-Box Attack Model Weijie Deng, South China Normal University, China Abstract-The random number generator (RNG) plays a crucial role in modern cryptography. While true RNG (TRNG) is available, pseudo RNG (PRNG) is often preferred due to its better compatibility. However, PRNGs have long been vulnerable to the leakage of internal states, which compromises their properties of resilience, forward security, and backward security. Furthermore, this threat will become more prevalent as adversaries gain full control of the PRNG. Inspired by whitebox cryptography, we aim to provide a definition of whitebox PRNG that protects against the leakage of internal states. Additionally, we bind the white-box PRNG with a specific application to resist code-lifting attacks. We implement the white-box PRNG based on various types of white-box SM4 ciphers, and measure their storage overhead and random number generation speed. Meanwhile, we evaluate the randomness of the generated numbers using randomness test standards, including NIST SP 800-90B and GM/T 0005-2021, and compare the testing results to the output of Linux entropy pool and OpenSSL-RNG.

ONLINE SESSION 4

SUNDAY, APRIL 23, 2023 Room A: 843 8802 8543

Online Session 4: Cloud Computing and Computer Network
Chairperson: Prof. Swathi Darla, SJB Institute of Technology/R V Institute of Technology and Management/Information Science and Engineering, India

09:40~09:55 SG507	Application of convolutional neural networks for the detection of diseases in theCCN-51 cocoa fruit by means of a mobile application Jerson Morocho, Universidad de las Fuerzas Armadas ESPE, Ecuador Abstract-CCN-51 cocoa, one of the two main varieties exported worldwide by Ecuador, due to the lack of technology and poor agronomic practices, is constantly attacked by a number of pests that affect its production, affecting the growth stages of the plant. Another factor that causes damage to the plant is the constant changes in climate, mostly due to excessive rainfall that causes an increase in humidity, damaging the flowering and fruit set, producing Moniliasis as one of its main diseases and being the crops far from the urban area, the analysis is time consuming and very costly, taking as an alternative for most producers the excessive use of chemicals to cure and maintain the pests and diseases of the plant. Where, this research project is proposed, consisting of developing a mobile application that by scanning images in a controlled environment allows the detection of diseases in the CCN-51 cocoa fruit. The mobile application will use its camera to scan the fruit and, using a trained image recognition model, predict a diagnosis of the disease present in the cocoa fruit.
09:55~10:10 SG509	Target Detection Algorithm of Forward Looking Sonar Based on Swin Transformer Lingyu Wang, Lingyu Wang, Ocean University of China, China Abstract-In recent years, with the deepening of the exploitation of Marine resources, the demand for Marine environment exploration is also increasing. However, due to the complex and changeable Marine environment, the exploration risk of under-water manned spacecraft is relatively high. Autonomous Underwater Vehicle (AUV) has become an essential tool to explore and exploit Marine resources. During the execution of underwater tasks, AUVs often encounter collision and entanglement of various obstacles, which will pose a fatal threat to AUVs. For-ward-looking Sonar (FLS) is one of the main sensors used by AUVs to detect underwater targets. By continuously transmitting sound waves and receiving echo signals, AUVs equipped with multi-beam forward-looking sonar can gener-ate real-time visual field acoustic images, and then detect the images with target detection algorithms to solve the above problems. However, the visual acoustic image has the characteristics of more texture feature information and less seman-tic feature information, and it requires real-time reasoning. Some existing classical target detection algorithms are mostly designed for some data scenes with strong semantic meaning, and cannot be well adapted to the visual acoustic image. Therefore, a new target detection algorithm, Swin_FLS, is proposed in this paper. The improved Swin_FLS can more fully extract the texture features in the for-ward-looking sonar image and adapt to the characteristics of the forward-looking sonar image data set. Finally, 85.2 mAP and 14.1 FPS are obtained in the test set. It surpasses the accuracy of some classical algorithms directly applied to the for-ward-looking sonar image data set.
10:10~10:25 SG512	Analysis of Bee Population and the Relationship with Time Muyang Li, Xiaole Liu, Chen Qi and Lexuan Liu, Amazingx academy, China Abstract-This essay proposes two methods to analyze bee populations in a given period. The first method is a quantitative analysis of the correlation between time and population, establishing a time-population model for bees. However, this method fails to provide a precise enough result. For improvement, the analysis of bee populations is augmented with more comprehensive factors (both positive and negative), creating a unified measure to calculate the total change in population percentage by assigning weights to each individual factor. During the construc-tion of these two methods, we completed the following five steps:Find relevant data with a numerical correlation between time and population: Data containing relevant information like time and population were

	downloaded from credible sources. Then, the data were fitted with linear regression to reveal the relationship between the population and time.Find possible factors that affect bee populations: External and internal factors were identified through a literature review of re-search articles and reputable online sources. Among these, five factors were deemed the most critical and to be used in this paper later.Assign weights to each factor through Entropy Weight Method (EWM) and Analytic Hierarchy Process (AHP): With EWM or AHP, a different set of weights was assigned to the fac-tors. However, in this paper, neither of these two was used alone. Instead, a uni-fied model that learns from both methods and hence generates a better weight for each factor is proposed and explained.Analysis of beehives needed to pollinate a 20-acre area: Parameters for the model were identified, defined, and populated us-ing relevant data. Finally, the minimum and the maximum number of beehives that satisfy the requirements were calculated and an average of the values was ob-tained.Testing of the model on Buhlmann 1985: With the fully calculated weights of different factors through the integrated method, the model was tested to see if the weight assignments were reasonable. To do this, the result obtained from this model is compared with data approached by Buhlmann (1985) as an evaluation of this model.
10:25~10:40 SG511	Internet of Things (IoT) enabled image segmentation model for Pneumonia detection: An approach based on Particle Swarm Optimization Suneet Kumar Gupta, Bennett University, Greater Noida, India Abstract-In the proposed article, all the intermediate steps involved for compression of UNet using PSO is well explained with suitable examples. Experimentally, it has been proven that the proposed algorithm compresses the architecture of UNet on chest X-ray dataset by 77% after 0.68% drop in accuracy with improvement in inference time by 2.23X.
10:40~10:55 SG513	Prediction of bee population and number of beehives required for pollination of a 20-acre parcel crop Yukun Jin, Tianyi Wei, Jingru Shi and Tingwen Chen, Amazingx academy, China Abstract-The decline of the bee population poses threats to the production of considerable types of crops that require pollination. The prediction of the bee's future population has therefore become a valuable research topic. For Problem one, we tried to solve it in mainly two ways: Using the Grey Forecast Model and using differential equations. For data that were missing, we process them by normalization at first, and then regress to find the abnormal data, and fill the missing data with average data after deleting abnormal data. For the Grey forecast, we use three types of models and compared their respective results with true values to pick the one with the most accurate output and use it to predict the population of bees. For the differential equation method, we simply express the rate of increase in population in terms of several variables (in the differential equation) and solve the equation to obtain the future population. For Problem two, we do a sensitivity test on the bee population. We applied the Random Forest model here to determine the im-portance of each variable. During the evaluation of the model, we test 4 sets of data and compare the Random Forest results with the true value. It turned out to be that the final model predicts the population precisely, which has proven that it is reliable. At last, we change the sensitivity of each variable for a 100% change and tell the importance of the variables. For Problem three, we get the model of the possibility of a plant being visited by a bee in a beehive system at any dis-tance, and then we use this matrix to simulate the area and calculate the possibility at any point. After determining a possible lower bound, we can get the area that can reach the bound which is the area the current beehive system can serve. By changing the number and the positions of beehives, we can get the maximum area the system can serve at any time. We can also calculate the possibility considering the planting density and the population of bees so it can be related to problem 1.
10:55~11:10 SG505	An optimized Deep Learning based Malicious Nodes Detection in Intelligent Sensor-Based Systems Using Blockchain Swathi Darla, SJB Institute of Technology/R V Institute of Technology and Management/Information Science and Engineering, India Abstract-In this research work, a blockchain-based secure routing model is proposed for Internet of Sensor Things (IoST), with the assistance acquired from deep learning-based hybrid meta-heuristic optimization model. The proposed model includes three major phases: (a) optimal cluster head

	selection, (b) lightweight blockchain-based registration and authentication mechanism, (c) optimized deep learning based malicious node identification and (d) optimal path identification. Initially, the network is constructed with N number of nodes. Among those nodes certain count of nodes is selected as optimal cluster head based on the two-fold objectives (energy consumption and delay) based hybrid optimization model (CMPRO). The proposed Chimp Social incentive-based Mutated Poor Rich Optimization Algorithm (CMPRO) is the conceptual amalgamation of the standard Chimp Optimization Algorithm (ChOA) and Poor and Rich Optimization (PRO) approach. Moreover, blockchain is deployed on the optimal CHs and base station because they have sufficient storage and computational resources. Subsequently, a lightweight blockchain-based registration and authentication mechanism is undergone. After the authentication of the network, the presence of malicious nodes in the network is detected using the new Optimized Deep Belief Network. To enhance the detection accuracy of the model, the hidden layers of DBN is optimized using the new hybrid optimization model (CMPRO). After the detection of malicious nodes, the source node selects the shortest path to the destination and performs secure routing in the absence of malicious node. In the proposed model, the optimal path for routing the data is identified using the Dijkstra algorithm. As a whole the network becomes secured. Finally, the performance of the model is validated to manifest its efficiency over the existing models.

ONLINE SESSION 5

SUNDAY, APRIL 23, 2023 Room A: 843 8802 8543

Online Session 5: Electronics Engineering

Chairperson: TBA

11:20~11:35 SG514	Vulnerabilities in Office Printers, Multifunction Printers (MFP), 3D Printers and Digital Copiers, A gateway to breach our enterprise network Eric Blancaflor, Mapua University, Philippines Abstract-Despite the advancements in security, threats have become more sophisticated than ever - leading companies to think outside the box. Cyber-attacks are becoming increasingly sophisticated due to hybrid work. Business continuity often took precedence over security concerns as organizations scrambled to comply with shifting regulations. Now that more people are working remotely via cloud services, IT needs assistance from cybersecurity experts. There are several sources that can pose a threat, including office printers. It is not uncommon for printers to have hundreds of potential entry points for hackers, who can then bring a system to its knees by taking control of one of the printers attached to it. In today's world, printers are very much computers and are often connected to the internet. Having advanced abilities makes it easy for cyber criminals to access them. This paper analyzes printer attacks from the past and provides a general methodology for analyzing printer security. Our methodology will be used to conduct online surveys of experienced IT practitioners to explore their exposure to social engineering attacks and security concerns related to printers, digital copiers, and 3D printers. Passive reconnaissance will be conducted to determine the extent to which some network protocols are exposed by these devices. A compiled checklist has been consolidated to be considered by businesses as a risk mitigation technique to secure the devices from vulnerabilities and attacks.
11:35~11:50 SG004	Speed Control of PMSM using Modified Particle Swarm Optimization Technique Based on Inertia Weight Updating Mechanism Raja Gandhi, NIT Meghalaya, India Abstract-In this paper, the modified PSO algorithm is imple-mented to tune the gain parameters of the PI speed controller of the PMSM drive system. The PSO algorithm is modified with the inertia weight updating mechanism to prevent premature convergence and balance the exploration and exploitation of the particles. The field-oriented vector control PMSM drive is developed in MATLAB/Simulink to examine three different conditions such as start-up, speed command change, and sud-den load torque imposition. The different parameters are then examined such as speed overshoot, settling time, peak time, rise time, and speed ripple, and the results are compared with conventional PSO-tuned PI controllers for the same motor. From the results, it is proved that the modified PSO-PI controller gives better performance compared to the conventional PSO-PI speed controller.
11:50~12:05 SG515	A Comparative Analysis of VPN applications and their Security Capabilities Towards Security Issues Jeremi An Armado, Mapua University, Philippines Abstract-In the current age, ensuring the security and confidentiality of information transmitted via the internet is a crucial issue for both individuals and companies, and plenty of technology companies and their technologies are offering such features. Like other numerous technologies, Virtual Private Networks (VPN) technologies have been applied to the modern world for security. Different VPN companies that offer free to paid services help provide security capabilities that a user would need to use when facing a vulnerability in using VPNs. These offers could include encryption, firewalls, and encryption with technologies such as tunneling, portal, and remote desktop architectures. This research has gathered information regarding user interest in VPNs, as well as seeking their confidence and knowledge regarding the security and privacy of different VPN clients. The results of the survey show that users are knowledgeable of VPNs, their services, and their acknowledgment of their vulnerability that

	hackers could use to their advantage.
12:05~12:20 SG005	Comparison of PSO and ACO Techniques with Speed Controller Tuning for DTC Controlled Induction Motor Drive Arpita Banik, NIT Meghalaya, India Abstract-To accomplish an optimized tuning of a PI controller in three-phase induction motor's direct torque control with space vector modulation (DTC-SVM), this study suggests two standardized optimization strategies called Particle Swarm Optimization (PSO) and Ant Colony Optimization (ACO) and compares, controls, analyses them with conventional method. These techniques are used for tuning of the proportional-integral (PI) controllers so that proper values of motor output parameters can be obtained in the DTC-SVM control loops. The goal of this study is to choose the most effective and reliable metaheuristic optimization approach from the two available options, PI-PSO and PI-ACO for DTC of IM. The MATLAB/Simulink platform is used to implement both proposed control systems, and simulation results are shown to support the strategy. The ACO-PI of DTC is giving great work performance for the IM system drive. The comparative findings between the suggested control method and the traditional DTC and PSO-PI revealed a considerable improvement in the control system. As a result, a highly accurate electromagnetic torque and speed estimate for calculating motor characteristics is produced.
12:20~12:35 SG516	Radio Frequency Identification Vulnerabilities: An Analysis on RFID-Related Physical Controls in an Infrastructure Jed Ivan Fiedalan, Mapua University, Philippines Abstract-Radio Frequency Identification (RFID) is a technology that uses radio waves to communicate between a reader and a tag attached to an object, to identify and track it. RFID systems consist of a reader, an antenna, and a tag or transponder [1]. In this research, the aim was to examine the vulnerabilities of RFID-related physical controls in an infrastructure, to identify potential vulnerabilities and assess the associated risks. The findings of this study will provide important insights into the current state of RFID-related physical controls in an infrastructure and will assist organizations in improving the security of their RFID systems.
12:35~12:50 SG006	Equivalent circuit for inverter fed induction motor control Rakesh Roy, NIT Meghalaya, India Abstract-This paper describes a method to determine the instantaneous input current, output power, input power factor and efficiency of sine PWM inverter fed induction motor using equivalent circuit. This method can be used for inverter fed induction motor with any PWM technique. The possible variation in all the parameters of induction motor equivalent circuit is also investigated and is compared with experimental results.

NOTE