

P027
15:00-15:15

DOSing Distributed Ledger Technology: IOTA

Mark A. Brady

University of Twente, Netherlands

Abstract-With advancements in connected technology, the number of ambitious applications involving Internet of Things (IoT) are drastically growing. This increases concerns related to security, scalability, and interoperability of IoT. As the network of connected devices grows, decentralized technologies become inevitable. Within this trend towards decentralization, distributed ledger technology (for instance IOTA) will be a significant driving force. IOTA is an innovative distributed ledger technology targeted towards low power devices, where energy efficiency is a high priority. Public research regarding security threats against IOTA especially denial-of-service (DoS) is essentially non-existent. In this paper we focus on exploring a DoS attack against IOTA. The proposed attack methodology takes advantage of the lack of fees along with the ability to transfer minuscule amounts. By sending many conflicting transactions as it results in a high number of re-attachments. The high number of re-attachments threatens IOTA's suitability for the IoT sphere. The implications of such attack, as well as the future of this issue in terms of the planned removal of the centralized coordinator are discussed.

P028
15:15-15:30

The Influence of Mobile Operation Systems on Mobile User Security Behavior

Martin J Butler

Stellenbosch University, South Africa

Abstract-Mobile security remains a concern for multiple stakeholders. Safe user behavior is crucial key to avoid and mitigate mobile threats. The research used a survey design to capture key constructs of mobile user threat avoidance behavior. Analysis revealed that there is no significant difference between the two key drivers of secure behavior, threat appraisal and coping appraisal, for Android and iOS users. However, statistically significant differences in avoidance motivation and avoidance behavior of users of the two operating systems were displayed. This indicates that existing threat avoidance models may be insufficient to comprehensively deal with factors that affect mobile user behavior. A newly introduced variable, perceived security, shows a difference in the perceptions of their level of protection among the users of the two operating systems, providing a new direction for research into mobile security. these methods. Finally, the developed models are reliable for not only the conceptual phase of future rural road projects but also the related construction fields can be recovered about the cost model creation.

for track utilization charges. In this study, the costs of infrastructure construction and maintenance on 5 route sections representing different traffic characteristics were studied by using records from 5 years. It was found that the maintenance cost of the telecommunication and signalling system ranges from 1.3 to 1.7 million baht per year per station. The average annual maintenance cost of the railway track was 280,000 to 310,000 baht per track per kilometre. The traffic density was found to be the main factor that influenced the maintenance cost.

P035
15:30-15:45

velink - A Blockchain-based Shared Mobility Platform for Private and Commercial Vehicles utilizing ERC-721 Tokens

Dominic Pirker
Graz University of Technology, Austria

Abstract-Transportation of people and goods is important and crucial in the context of smart cities. The trend in regard of people's mobility is moving from privately owned vehicles towards shared mobility. This trend is even stronger in urban areas, where space for parking is limited, and the mobility is supported by the public transport system, which lowers the need for private vehicles. Several challenges and barriers of currently available solutions retard a massive growth of this mobility option, such as the trust problem, data monopolism, or intermediary costs. Decentralizing mobility management is a promising approach to solve the current problems of the mobility market, allowing to move towards a more usable internet of mobility and smart transportation. Leveraging blockchain technology allows to cut intermediary costs, by utilizing smart contracts. Important in this ecosystem is the proof of identity of participants in the blockchain network. To proof the possession of the claimed identity, the private key corresponding to the wallet address is utilized, and therefore essential to protect. In this paper, a blockchain-based shared mobility platform is proposed and a proof-of-concept is shown. First, current problems and state-of-the-art systems are analyzed. Then, a decentralized concept is built based on ERC-721 tokens, implemented in a smart contract, and augmented with a Hardware Security Module (HSM) to protect the confidential key material. Finally, the system is evaluated and compared against state-of-the-art solutions.

P037
15:45-16:00

Lightweight Blockchain-based Platform for GDPR-Compliant Personal Data Management

Cristòfol Daudén-Esmel
Universitat Rovira i Virgili, Spain

Abstract-New digital technologies generate large amounts of information. This data is processed by Service Providers in order to improve and develop new services or products, but also to fund themselves. However, processing these personal data can result in the extraction of sensitive information.

In consequence, it can lead to users' privacy risk. To mitigate this risk, the EU elaborated the GDPR. It forces Service Providers to have Data Subjects' explicit consent for collecting and processing their personal data. The problem is that legislative text does not define how to transparently demonstrate that they already have this consent. Also, most users do not know the rights they have over their personal data, neither this regulation provides techniques for them to be aware about what happens with it. In this paper, we propose a lightweight blockchain-based GDPRcompliant personal data management platform. It provides public access to immutable evidences that show the agreements between the Data Subjects and Service Providers. The Service Providers can demonstrate that they are fulfilling the regulation, and Data Subjects are aware about what happens with their personal data and can manage it according to their rights.

P036
16:00-16:15

Assessment of Remote Biometric Authentication Systems: Another Take on the Quest to Replace Passwords

Daniel Köhler

Hasso Plattner Institute, Germany

Abstract—Passwords are often criticized due to being prone to misuses such as bad password creation and management practices. Experts usually advise using other forms of authentication. While there are plenty of alternative authentication methods available, an overall assessment often proves to be challenging. This is because of aspects such as differences in security techniques, different applicability of the system, or varying difficulties of implementation. To tackle the issue of comparing different authentication systems, unified criteria are needed. Bonneau et al. proposed a framework for comparing authentication schemes in their "The Quest to Replace Passwords". We contribute to the quest by providing information and assessment on the previously unassessed Remote Biometric Authentication Systems, thus increasing the variety of analyzed systems. We achieve this by analyzing six exemplary implementations. To enable proper evaluation of the details of that new category of authentication schemes, this work furthermore expands the framework by the two aspects Resilient-to-Biometric-Loss and No-Trusted-Execution-Environments.

P013
16:15-16:30

Detecting Android Malware Based on Dynamic Feature Sequence and Attention Mechanism

Hanlin Long

Harbin Institute of Technology (Shenzhen), China

Abstract-The mechanism of running software on virtual machines partly ensures the security of Android system. However, with all kinds of malicious codes being developed, there has been a huge number of massive security incidents caused by malware on Android. Malware has various code patterns, but their behaviors are measurable. In this paper, a new method of detecting Android malware by analyzing malware's behaviors is proposed. The method is characterized by the ability to mine the contextual relationships between system calls and network activities. Besides, the method requires only a small data set to achieve good classification performance.

We propose a set of methods for automatically collecting and organizing dynamic features from Android application Based on the collected features, deep neural network is used to classify software samples. We validate the effectiveness of the proposed method on a set of 2210 applications obtained from Androzoo. The experimental results demonstrate that the proposed method has high detection accuracy against wild malware as compared with other methods.

P034
16:30-16:45

A Study on Privacy Issues in Internet of Things (IoT)

Mayasarah Maslizan

Cybersecurity Malaysia, Malaysia

Abstract-Internet of Things (IoT) is an interconnected wireless network where smart nodes (IoT devices) interact with each other in order to exchange data through the communicating medium. Internet of Things (IoT) have rapidly increased in popularity, demand and commercial availability within the past several years. Various IoT applications generate a huge amount of data from different types of resources, including smart cities, manufacturing industries, health institutions, and governments. Due to the pervasive nature of IoT and the limitless opportunities that this technology provides, security and privacy becomes two key concerns for the users of these smart offerings. Most of the privacy threats disclosing the private information to unwanted party and gives rise to serious implications in various IoT application. Thus, this paper will analyse existing literature related to various privacy threats in IoT, privacy issues in different applications of IoT and present summary of the study.

Virtual Session 2: Computer and Intelligent Computing

Chair: Dr. Chau Kien Tsong, Universiti Sains Malaysia, Malaysia

Time: 14:30-17:15, January 9

Online Room: A3 *Link: <https://zoom.com.cn/j/67812626226> ID: 678 1262 6226*

P023
14:30-14:45 **Forensic Analysis of Binary Structures of Video Files**
Md Abir Hasan
University of Alaska Fairbanks, USA

Abstract-As technology advances, multimedia files such as videos are susceptible to manipulation. This has led to serious concerns that images and videos are not trustworthy evidence as the files can be manipulated easily. As a result, forensic analysis of electronic multimedia files plays an important role in verifying the authenticity of video files. This paper provides comprehensive details of a binary file forensic analysis technique for different media file containers, mostly focused on AVI and MP4/MOV container format. We also provide a considerable number of details to identify a forgery among video files. We present pivotal parameters which need to be tested to authenticate a video file. By analyzing the binary data structures and metadata, we can detect the use of editing tools, verify the purported source of a video file, and identify the true acquisition device model.

P001
14:45-15:00 **Trend Analysis and Countermeasure Research of DDoS Attack under 5G Network**
Haiou Huang
College of Computer Science and Technology, Jilin University, China

Abstract-DDoS has been terrorizing network operators since its birth in the late 20th century, and people are constantly researching new methods and techniques to mitigate or solve DDoS attacks. However, with the network technology update iteration, DDoS attacks also emerge in endlessly. When we exclaims the high speed experience brought by 5G, we should not forget that the network is a double-edged sword, and the security problem of 5G network is also not to be underestimated. As traditional DDoS defenses continue to fail, researchers who have grown more aggressive in recent years have seen some promising, low-cost technologies emerge. This paper first analyzes the trend of DDoS attacks in the past two years, then analyzes some DDoS defense mitigation schemes based on SDN, NFV and MTD, and points out some challenges faced by using new technologies to defend DDoS attacks.

P0012
15:00-15:15

Vehicle Flow Detection Based on Improved Deep Structure and Deep Sort
Haobin Li
Sichuan University, China

Abstract-Real-time vehicle detection based traffic monitoring is a hot research topic within the area of computer vision. In view of the problem of low detection accuracy and low processing speed, a vehicle detection method based on Improved Deep Structure is proposed in this study. Due to the characteristics of highway vehicles with a fixed aspect ratio, k-means ++ clustering method is used to select new anchor boxes to eliminate false targets at an early stage followed by improved depth structure with deep sort. Experimental results demonstrated that our proposed method on standard data set KITTI-UA achieved higher precision and faster speed than the existing algorithms.

P007
15:15-15:30

A Scheme of Key Distribution in Smart Grid
Youwu Zhou
State Grid JiangXi Electric Power Research Institute, China

Abstract-Group communication for Smart Grid, because of its special characteristics of large-scale nodes, open communication channel and high packets loss rate, making secure group communication of Smart Grid face many security threatens, so how to realize secure communication between groups and how to establish secure session keys shared between nodes has been the focus of Smart Grid. Aimed at the problem mentioned above, a group key distribution scheme based on three hash chains is proposed for Smart Grid. This scheme introduces a self-healing hash chain based on two-way hash chain, when a node is revoked, the corresponding self-healing hash value will be replaced by a new random value, so that revoked nodes can't realize collusion attack with the newly added node; This scheme also takes into account the problem of high packet loss rate in Smart Grid, and realizes self-healing property. The security and performance analysis shows that the scheme can meet the security requirements of group communication for Smart Grid, and it has the characteristics of dynamic revocation and resisting collusion. The scheme also reduces the storage overhead and the communication load of node to a large extent, and can meet the performance requirements of group communication for Smart Grid.

P025
15:30-15:45

Trust Evaluation Algorithm based on Association Rule Extraction
Ansheng YIN
Nanjing University of Posts and Telecommunications, China

Abstract-The current trust network evaluation models are mainly based on nodes' behavior, multi-attribute decision-making method or nodes' reputation. Due to the ambiguity and roughness of trust, these methods cannot express the trust of nodes well. Rule set matching algorithm can effectively deal with the ambiguity and roughness of trust. As the scale of the network expands and time increases, the scale of the trusted rule set will continue to grow, and at the same time, some of the rules collected may be invalid or even wrong. This paper proposes a rule extraction algorithm based on inclusion to improve the effectiveness and accuracy of rule set matching. Experimental results show that the algorithm is effective.

P0010
15:45-16:00

Correlation Filters with Pre-position by Reconstruction Error for Visual Tracking
Shengxiang Hu
Nanjing University of Science and Technology, China

Abstract-Correlation filter based on deep neural network is a kind of mainstream method for real-time object tracking. It combines the high efficiency of correlation filtering and the great representation ability of convolutional neural network. However, this method inherits most shortcomings of correlation filter such as boundary effects. If an object is close to the boundary of a search area due to a large displacement, the useful information will be filtered out by cosine window and padding. In order to alleviate boundary effects, we propose a coarse positioning module to fine tune the search area before cosine window and padding. The core of the proposed module is saliency detection based on reconstruction error. This enables the improved trackers to retain more object information than the prototypes. Experimental results show that our method obviously promotes the baseline model, namely DCFNet, in the case of fast motion. Due to the low computational cost of our coarse positioning module, the improved trackers still have real-time rate.

P2003
16:00-16:15

Document Fragments Restoration via Similarity Measurement

Liu Yuelan

Harbin Normal University, China

Abstract-The automatic restoration technology of shredded paper is an important branch in computer science. It plays an important role in judicial evidence restoration, the restoration of secret documents, and many other areas. In this article, we establish a similarity measurement model by data mining. This article mainly focuses on Chinese text files with regular cutting. The mathematic model is established and used for restoration, we provide several measurements to achieve the restoration and reduce the workload of manual intervention. At the same time, this article provides a way to restore two-side printing shredded documents. This paper gives experimental results that prove the effectiveness of the proposed method.

P021
16:15-16:30

Investigating the Compliance of the GDPR: Processing Personal Data on a Blockchain

Sarfraz Iqbal

Linnaeus University, Sweden

Abstract-Blockchain is a relatively new technology which needs to comply with the General Data Protection Regulation (GDPR) when processing personal data. In this study, the researchers focus on the issue of whether or not a blockchain that processes personal data can comply with the GDPR. Subsequently, it is important to discuss the advantages and disadvantages of using a blockchain from a civilian's point of view, since it is their personal data that will be processed. Finally, the results of a literature research and multiple interviews, show that there is no unequivocal answer to the compliancy issue regarding blockchains. This study contributes by extending the ongoing discussion on the topic of GDPR compliance on blockchain by showing that two different tendencies exist: purists and fundamentalists. Purists believe that public blockchains are the only 'real' blockchains and because of the characteristics those possess, it can never comply with the GDPR. Furthermore, all technical measures that try to comply with the principles of the GDPR will compromise the very existence of that blockchain. On the other hand, fundamentalists argue that it is possible to take certain technical measures to meet the requirements of the GDPR and these will not jeopardize the blockchain.

P2004
16:30-16:45

Research of Advertisement performance measure system based on Apache Flink and AB testing

Liu Yuelan

Harbin Normal University, China

Abstract-Nowadays due to the rapid growth of the internet, more and more websites or online applications are created to help people live a more convenient life. The main revenue source for these websites and online applications are through advertisements revenue. It has been a really hot topic recently regarding how to increase advertisements revenue through a better Ads designs that are more attractive to users. This paper researched on a real time Ads performance measure system based on apache flink that can effectively measure Ads performance 15 minutes after the Ads started. We also implemented this system in the paper as well.

P038
16:45-17:00

Automatic Test Case Generation for Vulnerability Analysis of Galois Field Arithmetic Circuits

Krishn Kumar Gupt

Limerick Institute of Technology, Ireland

Abstract-The research work proposes a framework for checking the correctness of Galois field arithmetic operations in digital circuits. The authors propose to automatically generate the test cases from the user input, avoiding reliance upon pre-designed test cases, comprising Galois field-width and respective choice of irreducible polynomial. We do this through the use of polynomial arithmetic to verify the circuits. To the best of author's knowledge, though extensive work has been carried out in optimising the performance of arithmetic operations in Galois field, there exist no testbench to evaluate the efficacy of hardware circuits incorporating this concept. By automating the process of generating test cases, the work can be scaled to test circuits of arbitrarily large field widths, thus providing a flexible architecture that guarantees correctness of the underlying design under test. We present simulation results for Galois field polynomials of width GF(22), GF(24) and GF(28). This work can be applied to test and prevent intentional tampering of data bit stream and safeguarding it against malicious activities, especially in applications such as cryptography that heavily relies on Galois field arithmetic.

P0019
17:00-17:15

The Effect of a Visual Novel Application on Students' Learning Motivation in Biology for Secondary School

Chau Kien Tsong

Universiti Sains Malaysia, Malaysia

This study investigates the capability of a genre of a digital game called "Grey Plague" visual novel in enhancing students' motivation in Biology. The content of the visual novel consists of Biology related topics taught in form four and five. This study was driven by the situation that many systems have failed to provide systematic understanding of the Biology concepts to the students. As such, the results of this research is of significance to students who wish to decide whether to use the visual novel in their Biology learning. Quantitative research utilising a set of questionnaires from 30 students had been conducted. The results of the user evaluation show that the mean scores for Learning Motivation and Aesthetics were 4.762 and 4.111 respectively. Aesthetics were also found positively correlated to Learning Motivation whereby the correlation values were 0.083. This concludes that the visual novel application is able to motivate and stimulate Malaysian science secondary students' interest to pursue their learning in Biology.

Virtual Session 3: Communication Network and Information Technology

Chairs: Prof. Shuangbao Wang, Morgan State University, USA

Dr. Abdulbast A. Abushgra, Cybersecurity Department, Utica College, USA

Time: 9:30-12:00, January 10

Online Room: B3 Link: <https://zoom.com.cn/j/61951443949> ID: 619 5144 3949

P019
9:30-9:45

Quantum Algorithms: Overviews, Foundations, and Speedup

Shuangbao Paul Wang and Eric Sakk

Morgan State University, USA

Abstract-This paper discusses quantum computing with a strong focus on quantum software, quantum networks, quantum simulation, and applications. The study on quantum speedups reveals fundamental differences between quantum algorithms and classical algorithms. As a case study, further improvement on Shor's algorithm is presented with experimental results. The study shows that quantum circuits can be generated automatically to further improve the efficiency of quantum algorithms.

P030
9:45-10:00

Damaged Fingerprint Recognition by Convolutional Long Short-Term Memory Networks for Forensic Purposes

Jaouhar Fattahi

Laval University, Canada

Abstract-Fingerprint recognition is often a game-changing step in establishing evidence against criminals. However, we are increasingly finding that criminals deliberately alter their fingerprints in a variety of ways to make it difficult for technicians and automatic sensors to recognize their fingerprints, making it tedious for investigators to establish strong evidence against them in a forensic procedure. In this sense, deep learning comes out as a prime candidate to assist in the recognition of damaged fingerprints. In particular, convolution algorithms. In this paper, we focus on the recognition of damaged fingerprints by Convolutional Long Short-Term Memory networks. We present the architecture of our model and demonstrate its performance which exceeds 95% accuracy, 99% precision, and approaches 95% recall and 99% AUC.

P017
 10:00-10:15

Code structures for quantum encryption and decryption

Eric Sakk

Morgan State University, USA

Abstract-The paradigm of quantum computation has led to the development of new algorithms as well variations on existing algorithms. In particular, novel cryptographic techniques based upon quantum computation are of great interest. Many classical encryption techniques naturally translate into the quantum paradigm because of their well-structured factorizations and the fact that they can be phased in the form of unitary operators. In this work, we demonstrate a quantum approach to data encryption and decryption based upon the McEliece cryptosystem using Reed-Muller codes. This example is of particular interest given that post-quantum analyses have highlighted this system as being robust against quantum attacks. Finally, in anticipation of quantum computation operating over binary fields, we discuss alternative operator factorizations for the proposed cryptosystem.

P024
 10:15-10:30

Analysis and Improvements to the Special Number Field Sieve for Discrete Logarithm Problems

Liwei Liu

Peking University, China

Abstract-The discrete logarithm problem(DLP) is a hard mathematical problem and a useful primitive in cryptography. A new computation record in a 795-bit prime field using the general number field sieve was completed recently, which approaches the widely used sizes like 1024 bit or even 2048 bit. However, such computations are always carried out to a safe prime, which brings people the notion that the safe prime with long bit-length is always "safe". In this paper, we fully analyze the variants of the number field sieve algorithm and employ a special number field sieve attack to a DLP computation in a 653-bit safe prime field. We propose a new method to find the special number field sieve(SNFS) polynomial pair of a given prime, and recommend a simple ad-hoc detection of the trapdoor before doing the general number field sieve(GNFS) to a prime p . We also give an experiment to show the huge difference between the cost of SNFS and GNFS. We think this work could justify some wrong thoughts about the security of cryptographic protocols based on prime field DLP and inspire more advanced methods for largerscale computation.

P032
10:30-10:45

SARG04 and AK15 Protocols Based on the Run-Time Execution and QBER

Abdulbast A. Abushgra

Cybersecurity Department, Utica College, USA

Abstract-Quantum computer has become a concern since the scientists have approved the ability of breaking the classical cryptographic methods in a potential Low-Run-Time Execution. The Run-Time could mean a risk for most of the classical algorithms; if not all. While the classical system depends on the sequential order of bits, quantum system will utilize simultaneous multi-channel submissions. These submissions can be used in several aspects of the quantum system, which include hardware, software, and applications. Also, the power of cryptographic algorithms is based on the processing machine or the Run-Time Execution (RTE). In cryptography, the preference usually is given to simple and fast processing algorithms, where in this paper will compare between two Quantum Key Distribution (QKD) Protocol algorithms. The comparison will discuss and demonstrate the Run-Time Execution between the SARG04 and AK15 Protocols, and both algorithms will be applied to the same number of qubits as well as the measurement mechanism. In addition, both protocols will be experienced to investigate the Quantum Bit Error Rate (QBER), and the possibility of the QBER occurs during qubits transmissions.

P020
10:45-11:00

Unified Attribute-Based Encryption Scheme for Industrial Internet of Things

Wei Li

Beijing Jinghang Computation and Communication Research Institute, China

Abstract-The Internet of Things (IoT) provides significant benefits for industry due to connect the devices together through the internet. Attribute-Based Encryption (ABE) is a technique can enforce an access control over data to guarantee the data security. In this paper, we propose an ABE scheme for data in industrial IoT. The scheme achieves both security and high performance. When there is a shared subpolicy among the access policies of a sensor, the scheme optimizes the encryption of the messages. Through analysis and simulation, we show that our solution is security and efficient. work provides an approach to fabricate a low-fouling membranes, which may find its application in protein separation and water treatment.

P015
11:00-11:15 SpaML: a Bimodal Ensemble Learning Spam Detector based on NLP Techniques
Jaouhar Fattahi
Laval University, Canada

Abstract-In this paper, we put forward a new tool, called SpaML, for spam detection using a set of supervised and unsupervised classifiers, and two techniques imbued with Natural Language Processing (NLP), namely Bag of Words (BoW) and Term Frequency-Inverse Document Frequency (TF-IDF). We first present the NLP techniques used. Then, we present our classifiers and their performance on each of these techniques. Then, we present our overall Ensemble Learning classifier and the strategy we are using to combine them. Finally, we present the interesting results shown by SpaML in terms of accuracy and precision.

P004
11:15-11:30 Multi-user broadcast authentication in Power LTE Private Network with Compressed Bloom Filter
Rui Liu^{1,2}

¹State Grid Electric Power Research Institute; ²Nanjing Nari Information Communication Technology Co., Ltd, China

Abstract-he number of Power LTE Private Network access terminals has increased sharply, which has impacted the traditional centralized authentication mechanism. In response to this problem, this paper proposes a lightweight and scalable multi-user broadcast authentication protocol. Compression cloth is used in multi-level μ TESLA, The Bloom filter replaces the process of binding the multi-level μ TESLA key chain by the Merkel tree. The protocol has properties such as long duration and self-healing. By allocating appropriate storage space at each receiving end, the communication load is greatly reduced. Combined with the Elliptic Curve Cryptography (ECC) algorithm similar to the public key cryptography (PKC) calculation mode, the analysis results show that the protocol can ensure long-term security and reduce energy consumption.

P031
11:30-11:45

DGA Domain Detection using Deep Learning

Haleh Shahzad

Telus, Canada

Abstract-Domain generation algorithms (DGAs) are used by attackers to generate a large number of pseudo-random domain names to connect to malicious command and control servers (C&Cs). These domain names are used to evade domain based security detection and mitigation controls. Reverse engineering of malware samples to discover the DGA algorithm and seed to generate the list of domains is one of the techniques used to detect DGA domains. These domains are subsequently preregistered and sinkholed, or published on security device blacklists to mitigate malicious activity. This technique is time-consuming and can be easily circumvented by attackers and malware authors. Statistical analysis is also used to identify DGA domains over a time window, however many of these techniques need contextual information which is not easily or feasibly obtained. Existing studies have also demonstrated the use of traditional machine learning techniques to detect DGA domains. Our goal was to detect DGA domains on a per domain basis using the domain name only, with no additional information. This paper presents a DGA classifier that leverages a recurrent neural network (RNN) based architecture for the detection of DGA domains without the need for contextual information or manually created features. We compared the performance of different RNN based architectures by evaluating them against a dataset of 2 million plus domain names. The results indicated little difference in performance metrics among the RNN architectures.

P029
11:45-12:00

Outage Performance of Satellite-UAV Network Framework based on NOMA

Xiangyu Yang

Henan Normal University, China

Abstract-A unified framework for UAV-aided satellite communication network based on non-orthogonal multiple access (NOMA) is proposed. The satellite serves as base station with the aid of a decode-forward (DF) UAV relay to communicate with two ground users using NOMA protocol. Assuming that there is no direct link between the satellite and users due to severe fading. The link of satellite-to-UAV is assumed to experience Rician fading and UAV-to-users are assumed to experience Nakagami-m fading. In order to evaluate the performance of the system model more directly, the expressions for the exact and asymptomatic outage probability at high SNR are derived. On the basis of these results, the system throughput under delay-limited transmission mode is obtained.

The correctness of theoretical deduction is verified by Monte-Carlo simulation. The simulation results show that: (1) NOMA performs better than traditional orthogonal multiple access (OMA) in terms of outage probability and system throughput. (2) The system performance of NOMA network is affected by the distribution fading parameter μ of Nakagami-m.

Virtual Session 4: Image processing technology and methods

Chair: Assoc. Prof. Lili Nurliyana Abdullah, Universiti Putra Malaysia, Malaysia

Time: 9:30-12:00, January 10

Online Room: A3 *Link: <https://zoom.com.cn/j/67812626226> ID: 678 1262 6226*

P0009
9:30-9:45

An improved SSD for small target detection

Xiang Li

Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang, China

Abstract-SSD is one of heuristic one-stage target detection approaches. Although it has got impressive results in general target detection, it still struggles in small-size object detection and precise location. In this paper, we proposed an improved SSD which forces on the small-size target detection. We include a shallow and high resolution feature into the hierarchical detection feature which are used for prediction. Then, we fuse the detection features (including the shallow and high resolution one) as a feature pyramid through some convolution layers and unsample operations to pass information from deep features to the shallow ones, aiming to enrich the semantic information of the shallow features. To make the network easier to converge, we add a L2 normalization to the bottom detection feature of the feature pyramid to make a norm balance between each pyramid feature. The experimental results on the VEDAI dataset show that the proposed method has obtained impressive progress than the original SSD for the small targets detection.

P010
9:45-10:00

Using Boltzmann Entropy to Measure Scrambling Degree of Grayscale Images

Xinghua Cheng

The Hong Kong Polytechnic University, Hong Kong, China

Abstract-Image data security is a key issue in storage, transmission. Many scrambling techniques have been developed to encrypt digital images. How to quantitatively measure the scrambling degree of images scrambled by various techniques is an issue. To address such an issue, this study proposes an evaluation scheme of scrambling degree from the perspective of thermodynamics. The whole image is considered as an isolated thermodynamics system where gas molecules are pixels. Specifically, Boltzmann entropy (thermodynamics entropy) is employed to measure the scrambling degree of scrambled images. The proposed scheme involves two levels (i.e., the plain image, bit planes). Four images are used in simulation experiments. The experimental results show that the proposed scheme is simple and effective in measuring the scrambling degree of grayscale images. This study indicates that Boltzmann entropy can be used to optimize the encryption of images.

P0013
10:00-10:15
Research on Behavior Recognition of Dairy Goat Based on Multi-model Fusion
Yi Li
Northwest A&F University, China

Abstract-In order to accurately identify the behavior of dairy goats in the image, a multi-model fusion convolutional neural network (CNN) method based on the image of dairy goats is proposed. At first, the AlexNet, ResNet50 and Vgg16 models are trained respectively, and the best recognition results of each model are obtained. Then, the attention weight of each model is calculated by feature stitching and other operations. Finally, The feature information of AlexNet, ResNet50 and Vgg16 is combined with attention mechanism to re-weight, and the parameters of the fused multi-model convolutional neural networks are adjusted to obtain the best recognition results of fusion models. Experimental results show that compared with single model and multi-model, the ARV fusion model we proposed achieves higher recognition accuracy, and the average accuracy of each dairy goat behavior is as high as 98.50%.

P0014
10:15-10:30
A Crowd Flow Segmentation Method based on Deep Motion Transformation Network
Qili Ni
Yangzhou University, China

Abstract-The crowd motion in public places is generally disorderly but locally orderly. Therefore, dividing the crowd flow into regions with basically consistent motion states can help us better understand and analyze the crowd's motion states. For this reason, a deep motion transformation network is proposed to segment the crowd flow into different motion states, which avoids the problem of parameter selection based on the clustering method. We test the method in different crowd density scenarios, and the experimental results show that the proposed method can achieve a better segmentation effect than the previous methods.

P0015
10:30-10:45

Tensor Inhomogeneous Average Sparse Matrix Based Texture Extraction
XIN JIN
Dalian Naval Academy, China

Abstract-Texture extraction is considered as a basic but a very challenging work in a lot of computer vision fields. Yet texture is not precisely defined, which is difficult to be separated from edges. In this paper, a novel texture extraction algorithm was proposed. Nonlinear structure tensor was introduced to distinguish textures out from edges. And an 8-neighborhood tensor inhomogeneous average sparse matrix was presented to smooth the images. The smoothness weights are determined by the local anisotropy. By applying this inhomogeneous average sparse matrix to the input images, the textures are smoothed to the detail layer while the edges are remained in the original images. The effectiveness of our method was demonstrated by the comparison results with other existing generally acknowledged texture extraction algorithms. And the sparse matrix framework reduces the computational cost than the convolution frameworks.

P0016
10:45-11:00

Blind Image Restoration and Super-Resolution for Multispectral Images Using Sparse Optimization
Yoshitaka Izumi
University of Tsukuba, Japan

Abstract-The purpose of this paper is two-fold. First, we extend the blind image deconvolution (BID) and blind super resolution (SR) methods developed in our previous work to multispectral images. Second, we introduce a new regularization technique called Patch-Based regularization in the BID and SR problems. This technique uses a low-rank property of image patches obtained by dividing each channel image as well as correlations in image intensity among different channels. We demonstrate performances of the proposed methods by simulation studies using images of a multispectral camera.

P0017
11:00-11:15

Registration between MVCT reconstructed from EPID and kVCT
Miaomiao Lu
Beijing Institute of Technology, China

Abstract-The registration of two-dimensional MV electronic portal imaging device (EPID) images and digital reconstruction radiograph (DRR) images has been widely used for the setup error correction of radiotherapy, the approaches estimate the 3D transformation is not very accurate. The purpose of this paper is to verify the feasibility of a new setup error estimation method that registers 3D planning CT image and 3D image that is reconstructed based on EPID. EPID images were acquired and used to reconstruct the MVCT by Algebraic Reconstruction Technique (ART) algorithm. The reconstructed image and the planning CT were registered by maximizing the mutual information (MI) between two 3D images. The registration error is less than 3mm, which is suitable for clinical implementation. The study demonstrated that the 3D/3D registration method proposed for the setup error correction of radiotherapy is feasible.

P0001
11:15-11:30

Analysis of Commodity image recognition based on deep learning
Shuyan Wang
Southwest Jiaotong University, China

Abstract-Deep learning has developed rapidly in recent years, especially in the field of image recognition. In this paper, the commodity recognition based on object detection method using deep convolutional neural networks is investigated. Firstly, the commodity image dataset in real-world retail product checkout situations is constructed. Then, the image data is trained via object detection deep networks. Finally, three representative deep learning methods involving YOLOv3, Faster R-CNN and RetinaNet are analyzed in detail. The experimental results show the effectiveness of our proposed approach.

P0011
11:30-11:45

Target Classification Algorithms Based on Multispectral Imaging: A Review

Zimu Zeng

Xi'an Institute of Optics and Precision Mechanics, Chinese Academy of Sciences, China

Abstract-Multispectral imaging extracts rich spectral information from targets, which greatly expands the function of traditional imaging technology. Multispectral imaging is widely used in agriculture, military, medicine, industry, and meteorology. Because of the information redundancy in multispectral images, it is necessary to reduce the dimension by pre-processing. In recent years, most of the researchers have adopted the methods of pre-processing before classification. Based on the principles of feature selection, feature transformation, and feature extraction, common dimensionality reduction methods are introduced, and the advantages and disadvantages of them are discussed. Afterwards, classification methods are divided into traditional methods and deep learning methods, and their characteristics and application prospect are discussed. Through comparison, the former are cost-effective and have the mature theories, while the latter have strong adaptability and high classification accuracy. At present, methods could be optimized from the perspective of saving computing resources and using spectral information efficiently. In the future, traditional methods will be improved and comprehensively used, while new methods with stronger adaptability and precision will be developed.

P2001
11:45-12:00

Lipid droplet recognition based on watershed algorithm and convolutional neural network

Shiwei Li

Southwest University, China

Abstract-Unbalanced storage and utilization of lipids in the liver can easily lead to non-alcoholic fatty liver, obesity and metabolic syndrome. Therefore, it is very significant to detect and classify lipids in cell pathology pictures. In order to achieve accurate identification of lipid droplets, we improved the watershed algorithm to achieve the segmentation of lipid droplets, and classified the lipid droplets based on transfer learning through a convolutional neural network. The experiment shows that the improved watershed algorithm is used to segment the lipid droplets and has achieved good results. The convolutional neural network transfer learning has achieved a classification accuracy of about 99%.

P2005
12:00-12:15

Research on UAV Image Mosaic Based on Improved AKAZE Feature and VFC Algorithm

QIAN-WEN LI

Xi'an University of Science and Technology Xi'an, China

Abstract-Aiming at the problem of low matching efficiency of traditional AKAZE algorithm, an improved algorithm is proposed that combines AKAZE and FREAK algorithms. First, AKAZE is used to extract feature points to ensure the accuracy of feature detection, and then the FREAK operator is used to calculate the descriptor, and then the VFC algorithm is used to perform accurate matching to improve the matching efficiency, and finally the weighted fusion algorithm is used to fuse the image. The research results show that compared with the traditional SIFT, the improved AKAZE algorithm improves the feature extraction time by about 1.11s, and the improved AKAZE algorithm in terms of computing descriptor efficiency increases the time by 1.32s than the SIFT and AKAZE algorithms, which can get higher The accuracy and matching results of the UAV realize rapid and seamless splicing of UAV images.

January 10-Sunday

8:50	Gather at Grand Nest Hotel' s lobby (Bus will leave at 9:00) <i>Address: No.11 Tangqi Road, Tangjia Wan, Zhuhai, Guangdong (广东省珠海市唐家湾唐淇路 11 号)</i>
10:00-12:00	Qinglv Road /Zhuhai Grand Theater/Zhuhai Fishing Girl <i>情侣路/日月贝/渔女像</i>
12:00-14:00	Zhuhai Beach Visiting & Lunch <i>海边泳场参观/自由午餐</i>
14:00-15:30	Hong Kong-Zhuhai-Macao Bridge Visiting by Cruise from Jiuzhou Port Terminal <i>九洲港码头游船 1.5h (横穿桥底, 近距离看港珠澳大桥)</i>
15:30-17:00	New Yuan Ming Palace <i>圆明新园参观</i>
17:00	Back to Grand Nest Hotel

Note:

Lunch is not included in the itinerary.

ID card/Passport is required.

