Guest Editorial Preface

Recent Research in Security, Privacy and Forensic Analysis System for Smart Devices

Gulshan Shrivastava, Sharda University, Greater Noida, India
Nhu Nguyen Gia, Duy Tan University, Vietnam
Loredana-Mihaela Stanciu, Politehnica University Timisoara, Romania
Dac-Nhuong Le, Haiphong University, Vietnam

In recent years, privacy and forensic analysis concerns with smart devices have become a key research area. The smart devices provide enhanced features such as optimized display, in-house health monitoring, people tracking, driving directions, etc. Smart device forensics analysis is a classification under digital forensics that mainly deals with the analysis of digital evidence found in smart devices such as smartphones, tablets and smartwatch. There is an enormous rate of increase in threats with constantly increasing releases of smart devices and hasty development in innovative technologies. Digital forensics analysis procedure to acquire and analyze digital evidence originated in a smart device based on file systems, logical memory storage and operating system architectures.

This special issue of the International Journal of Digital Crime and Forensics (IJDCF) contains five papers, which cover a range of aspects of security, privacy and forensic analysis system for smart devices, from case studies in the forensic investigation on common drone to the palmprint recognition and un-trusted user's analysis, as well as discussions on Safety of women. Each of these papers has undergone full double-blind peer review, prior to being selected for this special issue.

The first paper 'Drones Forensics: A Case Study of Digital Forensic Investigations Conducted on Common Drone Models' by Khalifa Al-Room, Farkhund Iqbal, Thar Baker, Babar Shah, Benjamin Yankson, Aine MacDermott and Patrick C. K. Hung contributed novel methodological approach for the digital forensic analysis of a seized drone. In this work, rapid evolution is found of multi-vendor drones in the market, and an increase in drone adoption for civilian applications. This possesses regulatory, safety, privacy, and security challenges, for law enforcement, when drones are involved in a crime; as standardized traditional digital forensic processes are not adept for conducting digital forensics investigations on drones. This investigation focused on six brands of drones commonly used in criminal activities and extracted forensically relevant data such as location information, captured images and videos, drones' flight path, and data related to the ownership of the confiscated drone. Al-Room et.al demonstrated challenges of law enforcement could rely on the proposed systematic process in evaluating drones in order to conduct sound forensic confiscation, data extraction, data analysis, in order to provide a meaningful and consistent result for different types of drones on the market. Although the six types of drones in this experiment are not the exhaustive list of drones, law enforcement can use this proposes a methodological approach, and standardized questionnaires

in conducting any drone forensic investigation to prove ownership, link the drone to the crime or previous crimes, show activities the device has been involved.

In the article 'Palmprint recognition using Hessian matrix and 2-component partition method' by Jyotismita Chaki and Nilanjan Dey thoroughly captures and analyzes the palmprint. It provides information on the epidermis raised portion containing the ridge structure, the ridge characteristics and the details of the ridge flow. Because of its permanence and uniqueness, it has also been used as a trusted medium for proof of user identity for more than a century. However, due to the restrictions in live scan methods and their computer abilities, it is gradually automated compared to other biometric policies. Palmprints may be utilized for terrorist, law enforcement or commercial purposes. The fundamental benefits of utilizing palmprint as an enticing biometric are its high distinguishability, constancy, high efficiency, low-resolution imaging, user-approachability, low price palm printing equipment, high stability, etc. The objective of the study is to build an efficient palmprint identification method from the principal lines. Because palm lines are distortion-free, it is quite trustworthy and can, therefore, be used to detect palmprints. The uniqueness of the proposed method involves the construction of a new technique for generating the region of interest (ROI) leading to a new principal line extraction method and texture matching. The new principal line extraction method is based on the Hessian matrix and the Eigenvalue. The ROI feature is extracted utilizing a new 2-component partition technique in which the principal lines are segmented into comparative and non- comparative lines. Palmprint image recognition is achieved by equating or matching the comparative and non-comparative lines between the training and test images.

Safety of women whether outside or at home is a priority nowadays. Dowry deaths, sexual harassment, abduction and kidnapping, rape and assaults are some of the common crimes against women. Sumit Kumar Yadav, Kavita Sharma and Ananya Gupta presented a new smart device technique for the safety of the elderly, children and especially women, which is more efficient and robust than the exiting techniques through the article 'SafeWomen: A smart device to secure women environment using ATmega328 with an Android Tracking app'. This device sends an alert along with an emergency message to the contacts that have been registered with the help of GPS and can be traced with the help of the IP address of the device whenever any unwanted incident is faced. This article has proposed improved technique as the existing devices pose limitations pertaining to their size, network connectivity, manual operation. This device is devised into three modes: Hardware, Smartphone and Integrated mode. The Hardware mode consists of a device with a button, buzzer, GPS module, facility to track the user/victim with the help of "Track User" feature. The button can be pressed when the user feels unsafe which activates the buzzer and the GPS module. The buzzer emits high pitched voice to get the attention of the people around, whereas the GPS module is used to send the emergency message to registered contacts. The Smartphone mode consists of deploying an android application on the phone which sends a notification to registered contacts by pressing the power button three times within two seconds or can be used to contact helpline numbers. The Integrated Mode is a combination of the hardware and smartphone mode to eliminate limitations such as network connectivity, handling of hardware that can be posed by the above mentioned two modes individually. With awareness and proper implementation of the idea behind SafeWomen, women can live freely without any fear and reach great heights in all arenas.

The article 'A Novel Verification Protocol to Restrict Unconstitutional Access of Information from Smart Card: A Novel Verification Protocol to Restrict' by Ajay Kumar Sahu and Ashish Kumar address the study evaluates recently recommended two-factor corroboration protocol for client-server system design and presented a novel solution to repress the existing anomalies. Analysis of two-factor corroboration suggests that it is unfortified under various circumstances. This article presents the merits and demerits of the currently used password-based verification protocols and proposed dynamic ID-based corroboration protocol supports mutual authentication and session key agreement, in which the communicating parties verify the legitimacy of each other and also compute the session key in cooperation. The recommended protocol fascinates all adorable security features, which are exhibited

in the security examination of the existing protocols. The security and achievement investigation of the proposed scheme suggests that it not only overwhelmed security susceptibility but also is extra influential than previous designs. Furthermore, Authors compared the proposed scheme with another relevant scheme to analyze the performance, illustrating that the endorsed system needs less time to execute significant operations and Crypto-Graphic operations. The comparison results justified that the proposed protocol is vigorous and cost-effective. Moreover, the simulating results of the recommended protocol using AVISPA software conclude that suggested protocol is safe against various possible attacks. Finally, concluded that suggested protocol is effectual to be implemented in real-life scenarios. The application of the presented scheme can be seen in areas where information leak is of utmost importance like medical, banking, defence and aeronautics etc. Therefore, the proposed scheme is ideal for deployment in low-power networks considering its low computational complexity, communication and storage costs.

In the last article of 'Detection of Suspicious or Un-Trusted Users in Crypto-Currency Financial Trading Applications' by Ruchi Mittal and M. P. S. Bhatia focuses on finding untrusted or suspicious users from the crypto-currencies management system network. Cryptocurrencies are the decentralized form of transactions which doesn't involve any third party, i.e. any banking system. Here, the authors proposed a methodology to investigate suspicious users from the who-trusts-whom network of people who trade using Bitcoin on a platform called Bitcoin OTC and Bitcoin Alpha. The proposed approach is a collaboration of the structural properties of social networks (Centralities and modularity class) and machine learning techniques (SVM, Random forest and so on). The experimental results conclude that users having a low score could be marked as an untrusted user. This approach helps to find malicious users form financial treading, which is connected via mobile apps, desktop applications and increase security walls for users who are treading on crypto-currency. The collaboration of machine learning techniques with social networks techniques improve the traditional methods for identifying untrusted users from financial applications

Finally, as editors of this special issue, we would like to thank all the reviewers for their excellent work and the authors for their contribution. We expect that International Journal of Digital Crime and Forensics (IJDCF) will provide the best platform for the authors and the readers, with a comprehensive overview of the most recent developments for security in network analytics and internet of things research.

Gulshan Shrivastava
Nhu Nguyen Gia
Loredana-Mihaela Stanciu
Dac-Nhuong Le
Guest Editors
IJDCF