Guest Editorial Preface

Special Issue on Advanced Digital Forensic Techniques for Digital Traces

Mamoun Alazab, College of Engineering, IT, and Environment, Charles Darwin University, Australia
Sivaraman Eswaran, Department of Computer Science and Engineering, PES University, Bangalore, India
Prasad Honnavalli, Department of Computer Science and Engineering, PES University, Bangalore, India

Nowadays there are huge volumes of data, heterogeneous information, and networking technologies. This creates a great challenge for security analysis including law enforcement agencies investigating cybercrime. Digital forensics is the scientific acquisition, analysis, and preservation of data using forensic equipment and special software tools. The objective is to locate, identify, collect, and acquire data. The stages of the digital forensics process require differing specialist training and knowledge. New emerging technologies make the digital forensic very challenging. The scope of this special issue encompasses the digital forensics of IoT, CPS, mobile systems, ITS, Blockchain, mobile networks, and mobile cloud, including but not limited to operating systems of Android, iOS and Windows Mobile, smartphones, and applications.

This special issue of the *International Journal of Digital Crime and Forensics* (IJDCF) received a total of 16 papers and out of which eight papers were accepted after revision from the authors. Eight papers will be included in the special issue. The eight papers in this special issue cover a range of aspects of advanced digital forensics techniques. Each of these revised papers has undergone full double blind peer review, prior to being selected for this special issue.

Ashok Kumar Mohan, Sethumadhavan Madathil and Lakshmy KV explore models such as Unique Pockets (UP), Unique Groups (UG), and Unique Association (UA) to address the exclusive challenges mixed up in identifying incoherent associations that are buried well within the meagre metadata field-value pairs. In the article "A New Framework for Matching Forensic Composite Sketches With the Digital Images," the authors conduct research on how face sketch recognition is considered a sub-problem of face recognition. They propose a new Convolution Neural Network (CNN) framework for this research. It is evaluated on two datasets and it exhibits an accuracy of 78.26% with Extended-PRIP (E-PRIP) and 69.57% with Composite Sketches with Age Variations (CSA) respectively. Experimental analysis shows the improved results compared state-of-the-art composite sketch matching systems.

The next article, "Behavioural Evidence Analysis: A Paradigm Shift in Digital Forensics," conducted research on Digital Forensics (DF) by using the study of behavioural clues based on Behavioural Evidence Analysis (BEA). The authors review existing BEA approaches and process models and concludes the lack of standardisation in the BEA process. This standard BEA framework classifies digital evidence into categories to decipher associated offender characteristics. Unlike existing models, this new approach collects evidence from diverse sources and leaves no aspect

unattended while probing criminal behavioural cues, thus facilitating its applicability across varied forensic domains.

In "Design and Development of Ternary-Based Anomaly Detection in Semantic Graphs Using Metaheuristic Algorithm," Sravan Kumar Reddy and Dharmendra Singh Rajput introduce a new optimization concept referred to Biogeography Optimization with Fitness Sorted Update (BO-FSU) to detect the abnormalities in the network nodes which is the extended version of the standard Biogeography Optimization Algorithm (BBO). The abnormal behavior in the network is identified by the similarities among the derived rule features. Further, the performance of the proposed model is compared over the other classical models in terms of certain performance measures. The authors claim that these techniques will be useful to detect digital crime and forensics.

Rajashree Soman and Sukumar R aim to provide a reliable and secure image sharing by building a novel cloud platform which is a secure storage in the public cloud. The main objective of their paper "Secure Storage and Sharing of Visitor Images Generated by Smart Entrance on Public Cloud" is to provide a new way of secure image data storage and transmission on cloud using cryptographic algorithms. To overcome the flaws in current system, a novel method using BigchainDB which has advantages of blockchain technology and traditional database is proposed for storing attributes of image.

In their paper "Holistic Analytics of Digital Artifacts Unique Metadata Association Model," the authors try to verify the existing similarity models and proposed unique mapping models by the Unique Metadata Association Model.

Rupa Ch, Sumaiya Shaikh and Mukesh Chinta has designed a framework to identify the concealed data in the multimedia file in the proposed system. This paper, "Multimedia Concealed Data Detection Using Quantitative Steganalysis," has strength to analyze concealed data images without embedding and extracting the image's payloads. A quantitative steganalysis approach was considered to accomplish the proposed objective. By using this approach, the authors were able to achieve results with 98% accuracy.

More Swami Das and A Govardhan propose a model for forensic application with the assurance of cloud log that helps the digital and cloud forensic investigators for collecting forensic scientific evidences. In their paper, "A Model of Cloud Forensic Application with Assurance of Cloud Log," they discuss the real-time dataset, network dataset results which lists the attacks with the highest attack type and also a case conducted chat log which will predict the attacks in advance by keywork ontology learning process, NLP and AI techniques.

In "Malevolent Node Detection based on Network Parameters Mining in Wireless Sensor Networks," Sunitha R and Chandrika J. design an exceptionally strong and effective evolutionary computing allied WSN routing convention for QoS and power effectiveness. The proposed routing convention includes proficient capacity called Network Condition Based Malicious Node Detection. The experimentation was carried out using network simulator tool NS2 and results ensure that the proposed routing model accomplishes higher throughput, low energy utilization, and low delay that sustains its suitability for real-time WSN.

It is our hope that this fine collection of articles will be a valuable resource for *International Journal of Digital Crime and Forensics* (IJDCF) readers and will stimulate further research into the vibrant area of digital forensics.

Mamoun Alazab
Sivaraman Eswaran
Prasad Honnavalli
Guest Editors
IJDCF