

Table of Contents

International Journal of Digital Crime and Forensics

Volume 12 • Issue 1 • January-March-2020 • ISSN: 1941-6210 • eISSN: 1941-6229

RESEARCH ARTICLES

- 1 The Internet of Things: Challenges and Considerations for Cybercrime Investigations and Digital Forensics**
Aine MacDermott, Liverpool John Moores University, Merseyside, UK
Thar Baker, Liverpool John Moores University, Merseyside, UK
Paul Buck, Liverpool John Moores University, Merseyside, UK
Farkhund Iqbal, Zayed University, Abu Dhabi, UAE
Qi Shi, Liverpool John Moores University, Merseyside, UK

- 14 A Novel Video Forgery Detection Model Based on Triangular Polarity Feature Classification**
Chee Cheun Huang, Institute for Infocomm Research, A*STAR, Singapore, Singapore
Chien Eao Lee, Institute for Infocomm Research, A*STAR, Singapore, Singapore
Vrizlynn L. L. Thing, Institute for Infocomm Research, A*STAR, Singapore, Singapore

- 35 Towards a Better Understanding of Drone Forensics: A Case Study of Parrot AR Drone 2.0**
Hana Bouaffif, ESPRIT School of Engineering, Tunis, Tunisia
Fauzi Kamoun, ESPRIT School of Engineering, Tunis, Tunisia
Farkhund Iqbal, College of Technical Innovation, Zayed University, Abu Dhabi, UAE

- 58 Evaluation of Autopsy and Volatility for Cybercrime Investigation A Forensic Lucid Case Study**
Ahmed Almutairi, Concordia University, Quebec, Canada
Behzad Shoarian Sattari, Concordia University, Quebec, Canada
Carlos Rivas, Concordia University, Quebec, Canada
Cristian Florin Stanciu, Concordia University, Quebec, Canada
Mozhdeh Yamani, Concordia University, Quebec, Canada
Zahra Zohoorasadat, Concordia University, Quebec, Canada
Serguei A. Mokhov, Concordia University, Quebec, Canada

- 90 A Deep Learning Framework for Malware Classification**
Mahmoud Kalash, University of Manitoba, Winnipeg, Canada
Mrigank Rochan, University of Manitoba, Winnipeg, Canada
Noman Mohammed, University of Manitoba, Winnipeg, Canada
Neil Bruce, Ryerson University, Toronto, Canada
Yang Wang, University of Manitoba, Winnipeg, Canada
Farkhund Iqbal, Zayed University, Abu Dhabi, UAE

- 109 A Hybrid Intrusion Detection System for IoT Applications with Constrained Resources**
Chao Wu, Chongqing Vehicle Test & Research Institute Co. Ltd., Chongqing, China
Yuan'an Liu, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, China
Fan Wu, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, China
Feng Liu, SKLOIS, IIE & SCS UCAS, CAS, Beijing, China
Hui Lu, Institute of Microelectronics of the Chinese Academy of Sciences, Beijing, China
Wenhao Fan, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, China
Bihua Tang, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, China

- 131 ENF Based Video Forgery Detection Algorithm**
Yufei Wang, South China University of Technology, Guangzhou, China
Yongjian Hu, South China University of Technology, Guangzhou, China & Sino-Singapore International Joint Research Institute, Guangzhou, China
Alan Wee-Chung Liew, Griffith University, Gold Coast Campus, Australia
Chang-Tsun Li, Deakin University, Geelong Campus, Australia

- 157 Reversible Data Hiding Based on Adaptive Block Selection Strategy**
Dan Huang, Guangdong Provincial Key Laboratory of Information, Security Technology, Sun Yat-sen University, Guangzhou, China
Fangjun Huang, School of Data and Computer Science, Sun Yat-sen University, Guangzhou, China

Copyright

The *International Journal of Digital Crime and Forensics (IJDCF)* (ISSN 1941-6210; eISSN 1941-6229), Copyright © 2021 IGI Global. From the journal's inception, January 1, 2009, to December 31, 2020, all rights, including translation into other languages is reserved by the publisher, unless otherwise stated in the article manuscript. As of January 1, 2021, this journal operates under the gold Open Access model, whereby all content published after this date is distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License (<http://creativecommons.org/licenses/by/4.0/>) where copyright for the work remains solely with the author(s) of the article manuscript. Product or company names used in this journal are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark. The views expressed in this journal are those of the authors but not necessarily of IGI Global.

The *International Journal of Digital Crime and Forensics* is indexed or listed in the following: ACM Digital Library; Applied Social Sciences Index & Abstracts (ASSIA); Bacon's Media Directory; Cabell's Directories; Compendex (Elsevier Engineering Index); DBLP; GetCited; Google Scholar; INSPEC; JournalTOCs; Library & Information Science Abstracts (LISA); MediaFinder; Norwegian Social Science Data Services (NSD); SCOPUS; The Index of Information Systems Journals; The Standard Periodical Directory; Ulrich's Periodicals Directory; Web of Science; Web of Science Emerging Sources Citation Index (ESCI)