Wireless Communications and Mobile Computing

WILEY | Hindawi

Special Issue on

Computational Intelligence Techniques for Information Security and Forensics in IoT Environments

CALL FOR PAPERS

As a popular paradigm, the Internet-of-Things (IoT) usually consists of numerous smart devices interconnected with other devices, application services, and systems by wireless networks and protocols. These smart devices often collect a massive amount of data from real-world objects via sensors and process, transmit and manage these data to networks for a variety of practical applications such as smart cities, smart homes, autonomous transportation, and health supervision. This raises two problems that must be addressed urgently; how to ensure the security of these IoT data, and how to implement the forensics of these data if they suffer illegal copying, tampering, and forgery attacks in IoT environments.

Computational intelligence techniques have shown the desirable efficiency and effectiveness in data processing and mining, and they have attracted a lot of attention. Recently, a typical example is deep convolutional neural networks (CNN) and its derivates, such as Faster Region-based CNN (Faster R-CNN) and Generative Adversarial Networks (GAN). These examples have gained great success in many basic computer vision tasks including automatic image representation generation, semantic segmentation and classification, object detection and tracking, and data restoration. They have outperformed traditional methods significantly. Due to the promising performances of computational intelligence techniques in data processing and mining tasks of computer vision, it might be reasonable and effective to explore these computational intelligence techniques to address the problems of information security and forensics in IoT environments.

The aim of this Special Issue is to solicit original research articles and review articles that focus on the challenges and issues of information security and forensics in IoT environments by computational intelligence techniques and models.

Potential topics include but are not limited to the following:

- Computational intelligence theories and methodologies for IoT data security
- Deep learning feature-based IoT data search
- Perceptual visual content representation, modelling, and understanding in IoT
- Privacy data control and management in IoT
- Steganography and steganalysis by Generative Adversarial Networks (GAN) or other deep learning networks in IoT
- Secret image sharing/visual cryptography by computational intelligence techniques in IoT
- Digital watermarking schemes by deep learning techniques in IoT
- Digital forensics by deep learning techniques in IoT
- Forensics of deep fake faces generated by GAN
- Fingerprint liveness forensics in IoT
- IoT copy data/tamper data detection by computational intelligence techniques
- Identity authentication in IoT
- Blockchain techniques for tamper-proofing of IoT data or other security applications

Authors can submit their manuscripts through the Manuscript Tracking System at https://review.hindawi.com/submit?specialIssue=760034.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Zhili Zhou, Nanjing University of Information Science & Technology, Nanjing, China
zhou_zhili@163.com

Guest Editors
Yimin Yang, Lakehead University, Thunder Bay, Canada
yyang48@lakeheadu.ca

James C.N. Yang, National Dong Hwa University, Hualien, Taiwan
cnyang@gms.ndhu.edu.tw

Cheonshik Kim, Sejong University, Seoul, Republic of Korea
mipsan@daum.net

Stelvio Cimato, University of Milano, Crema, Italy
stelvio.cimato@unimi.it

Gaurav Bhatnagar, Indian Institute of Technology, Jodhpur, India
goravdma@gmail.com

Submission Deadline
Friday, 18 December 2020

Publication Date
May 2021