Guest editorial

Editorial of special issue on information security and biometrics

As the advances of information technology, an enormously volume of data is available in different areas, and the capacity to electronically store, transfer and process those data continues to grow exponentially. Accordingly, issues such as information security and data privacy are more challenging, especially when combined in cyberspace. For example, large volume of data provides the potentials to identify personal sensitive information through privacy attacks together with simple background knowledge. This serious violation may not be easy to implement previously but become possible in the Big Data era. On the other hand, Biometrics are the emerging measure to quantify a person using his/her biological properties such as finger print, face, retina, DNA. To perform any experiment using information security, feature extraction and classification are potentially empowered by the biometrics. The field of biometrics normally does not go independently, and it is also possible to emulate security features of biological properties.

Based on the submissions in "International Conference on Applications and Techniques in Information Security (ATIS 2018)" and an open call for papers procedure, we selected 5 representative research articles for publication after rigorous peer-review processes. Towards those above-mentioned challenges, these articles propose promising solutions and excellent literature reviews for information security and biometrics. Here, we provide an integrative perspective of this special issue by summarizing some of the contribution contained therein.

Palmprints, compared with other biometric modalities, satisfy the critical properties of biometric characteristics such as universality, individuality, stability and collectability. But for images taken from low-cost devices, how to make the systems efficient and effective calls for some promising alternative biometric authentication. Taouche and Belhadef (2019) proposed to use multimodal biometrics by combining left and right palmprints of an individual into an authentication system. New feature descriptors, MB-LDP, MB-ELDP and MB-LDN are proposed, and then the GA and BSA are applied to do feature selection. Their prototype system and empirical results show that those new features bring the boost of performance in terms of recognition rate.

For online data exchange, sensitive information needs to be protected and transferred by using a reliable mechanism. Entity authentication in wireless networks is challenging for resource constrained devices such as mobile phones, because this process involves the complex computation. In Prakasha *et al.* (2019), proposed an enhanced authenticated key agreement scheme by incorporating fast cryptographic algorithms. Entity authentication is often coupled with the distribution of "session key" with the communicating entity, and the session key generated is used later to achieve confidentiality and integrity. The formal validation of the proposed scheme using AVISPA shows that the scheme is safe and secure from potential attacks. The performance evaluation of the proposed method depicts that it also increases the speed of authentication process.

For video surveillance, maintaining the captured videos usually calls for background modelling, which has played an imperative role in the moving object detection as progress of foreground extraction during video analysis. Shahidha and Maheswari (2019) proposed a background modelling technique that exploits the region-based background subtraction. It also provides quick response to the real-time scenario with data inconsistency. Furthermore, RRH algorithm is introduced to model the background that selects the specific region in a faster manner and promotes efficient foreground segmentation. Their experimental result shows that the proposed mechanism works well in most situations with varying conditions.

Although in this special issue significant efforts have been made from the perspectives of different area of information security and biometrics, we should note that many other exciting areas such as data privacy and privacy-aware learning are also worthy of being explored in future. Before the end of this editorial, we would like to thank the anonymous reviewers for their great efforts in reviewing the submitted manuscripts; without them this special issue would not have been published with such high quality. We would also like to thank the editor-in-chief office of *Information Discovery and Delivery* for their supportive guidance during the whole process in the organization of this special issue.

Gang Li
School of Information Technology, Deakin University, Melbourne, Australia

Srikanth Prabhu
Manipal Academy of Higher Education, Manipal, India

Qingfeng Chen
Guangxi University, Nanning, China, and

Jia Wu
Department of Computing, Macquarie University, Sydney, Australia

References

Prakasha, K., Muniyal, B. and Acharya, V. (2019), "Enhanced authentication and key agreement for end to end security in mobile commerce using wireless public key infrastructure", *Information Discovery and Delivery*, Vol. 1.

Shahidha, B.S. and Maheswari, N. (2019), "An effective foreground segmentation using adaptive region based background modelling", *Information Discovery and Delivery*.

Taouche, C. and Belhadef, H. (2019), "Multimodal biometric system combining left and right palmprints", *Information Discovery and Delivery*, Vol. 1.

The current issue and full text archive of this journal is available on Emerald Insight at: **https://www.emerald.com/insight/2398-6247.htm**

Information Discovery and Delivery
48/1 (2020) 1
 [ISSN 2398-6247]
[DOI 10.1108/IDD-02-2020-085]