New Advances of Privacy Protection and Multimedia Content Security for Big Data and Cloud Computing

Multimedia signal processing and Internet technology are popular in our daily lives. However, a lot of security problems have emerged correspondingly, including covert communication using multimedia files, copy-move forgery in digital images and videos, and biometric attacks. To address these problems, many techniques about multimedia information security were proposed by using the methods such as steganography, watermarking, encryption, privacy protection, and deep learning. Nevertheless, there are still some obvious shortcomings in research methodologies. Current studies for multimedia content security are usually based on strict conditions that are nearly impossible to be satisfied in real applications. Furthermore, high computation complexity of the current methods makes it difficult to handle the big data in the cloud computing environment. All these drawbacks limit the real applications of these techniques for multimedia security, and deserve additional in-depth investigations.

This special issue will focus on the latest research on the topics of privacy protection and multimedia content security, with a particular emphasis on novel and highly efficient methods that have the potentials to be applied for big data. According to the rigorous review procedure, each manuscript submitted to this special issue was technically reviewed by at least three anonymous experts in several rounds. Finally, twelve papers were selected to be included in this special issue, which fall into four main categories: (1) Steganography (six papers), (2) Privacy Protection (two papers), (3) Encryption (two papers), and (4) Attack (two papers). In the following paragraphs, we introduce these papers briefly.

1. STEGANOGRAPHY

The paper, entitled “A Robust Image Steganography on Resisting JPEG Compression with No Side Information”, first analyzes the error diffusion of steganographic embedding encoder, and then proposes a robust steganography with no side information based on the error diffusion analysis result and the relationship between DCT coefficients. The results based on BOSSbase 1.01 image library show that this method can resist JPEG compression effectively with acceptable robustness to steganalysis statistical detection. Different with conventional works, the paper, entitled “Constructive Steganography Using Texture Synthesis”, propose to construct an intermediate texture before data hiding, thus, more candidate patches can be utilized to carry secret bits during texture synthesis with better quality of synthesized image. The paper, entitled “A Coverless Information Hiding Algorithm Based on Grayscale Gradient Co-occurrence Matrix”, uses the grayscale gradient co-occurrence matrix to encode images and utilizes the mapping relationship between images and random numbers to express payload information. Experimental results show that this algorithm can be tolerant to JPEG compression and low-pass filtering. The paper, entitled “Data hiding in Iris Image for Privacy Protection”, restricts the modifications of the embedding within the regions that seldom affects iris recognition with the assist of syndrome trellis coding (STC), and a new distortion function is presented to measure the impact of data embedding, where the regions with important iris features are assigned with high embedding cost. The paper, entitled “Anti-HEVC Recompression Video Watermarking Algorithm Based on the All Phase Biorthogonal Transform and SVD”, embeds watermark in the quantized coefficients based on high efficiency video coding (HEVC) compression domain, which can decrease cumulative errors. In order to resist recompression attack, based on the all phase biorthogonal transform (APBT) and SVD, an anti-HEVC recompression video watermarking scheme is proposed. The paper, entitled “RTP Timestamp Steganography Detection Method”, realizes timestamp-based least significant bit (LSB) steganography detection, and a clustering analysis of the area between the 5th degree polynomial best-fit curves with different message windows is conducted with high accuracy in the 2nd round of clustering.

2. PRIVACY PROTECTION

The paper, entitled “The Location Privacy Preserving of Social Network based on RCCAM Access Control”, © 2019 The Author(s). Published by Informa UK Limited trading as Taylor & Francis Group on behalf of © The Institution of Electronics and Telecommunications Engineers (IETE). This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.
aims to solve the risk problem of location privacy disclosure in social network. Based on RCCAM access control model, a location privacy preservation scheme is proposed to assign accessing users of access permission and visibility level through the combined strategies of conflict resolution, permission allocation and location generalization. The paper, entitled “A Privacy-Preserving Image Retrieval Method Based on Improved BoVW Model in Cloud Environment”, proposes a privacy-preserving image retrieval method, which uses an improved bag of visual words (BoVW) model based on Hamming embedding and orthogonal transformation to provide binary signatures refining the matching of visual words with privacy preserving at the same time.

3. ENCRYPTION

The paper, entitled “Efficient Fully Homomorphic Encryption with Large Plaintext Space”, optimizes the rounding function of decryption procedure in Ducas and Micciancio’s scheme, called as FHEW, and then designs an algorithm for extracting the most significant digit of external ciphertext by employing the homomorphic accumulator, which can enlarge the plaintext space effectively. The paper, entitled “An IBE Scheme with Verifiable Outsourced Key Generation Based on a Single Server”, proposes an identity-based encryption scheme where the private key generation (PKG) outsources the task to a single server, and the results can be verified effectively. The PKG only requires the execution of one modular exponentiation, therefore, the total computing time of PKG and the server in the outsourcing algorithm is far less than that of direct computation.

4. ATTACK

The paper, entitled “An Attack on Hollow CAPTCHA Using Accurate Filling and Nonredundant Merging”, proposes an attack method on hollow CAPTCHA through accurate filling and non-redundant merging, in which the operations of thinning, inner-outer contour filling, segmentation, minimum-nearest neighbor merging and convolutional neural network (CNN) are involved. Results show that this method has higher success rate and superior efficiency compared with some existing attack methods on hollow CAPTCHA. The paper, entitled “Exploration for Software Mitigation to Spectre Attacks of Poisoning Indirect Branches”, claims that the pure software fix does impact on performance to existing software but varies depending on how the applications interact with the kernel, and the more a program relies on the kernel, the greater regression it shows. In order to alleviate this impact, a method that uses user space network stack is proposed in this paper, which is also evaluated by the fast packet I/O framework.

The publication of this special issue was achieved based on sincere cooperation. The Guest Editorial team would like to thank all the authors for the submission of their excellent works and also appreciate the technical reviewers for their precious time and hard work in reviewing. We also extend our appreciations to the IETE and Taylor & Francis staffs, especially Mrs Sandeep Kaur Mangat, for their kind and careful work. We do hope that the twelve papers published in this special issue of IETETR could benefit the readers especially the young researchers with wider range of information and better understanding in the field. Specially, we would like to deeply thank Prof M Jagadesh Kumar, Editor-in-Chief of IETE Technical Review, for his great support and guidance from the beginning to the eventual publication of this special issue.

GUEST EDITORIAL TEAM

[Chuan Qin]: Dr Chuan Qin has been with the faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology since 2008, where he is currently a Professor. He received the BS and MS degrees from Hefei University of Technology, China, in 2002 and 2005, respectively, and the PhD degree from Shanghai University, China, in 2008. He was with Feng Chia University at Taiwan as a Postdoctoral Researcher from July 2010 to July 2012. He has served as the Editorial Board Member, Associate Editor and Editor for a lot of international journals, and also organized six special issues. He has been the technical reviewer for some famous journals, such as IEEE Trans. on Image Processing, IEEE Trans. on IFS, and IEEE Trans. on CSVT. His current research works are supported by the Natural Science Foundation of China. His research interests include image processing and multimedia security. He has published more than 100 papers in these areas.

[Zhenxing Qian]: Dr Zhenxing Qian has been with the faculty of the School of Communication and Information Engineering, Shanghai University since 2009. Now, he is a Professor of Fudan University. He received both the BS and the PhD degrees from University of Science and Technology of China (USTC) in 2003 and 2007, respectively. He has published over 80 peer-reviewed papers on international journals and conferences, and has managed more than 10 projects including three projects of National Science Foundation of China and the Shanghai Rising-Star Project. His research interests include information hiding, image processing and multimedia security.
[Jinwei Wang]: Dr Jinwei Wang is working as a professor at Nanjing University of Information Science and Technology, China. He was born in Inner Mongolia, China, in 1978. He received the PhD degree in information security at Nanjing University of Science & Technology in 2007 and was a visiting scholar in Service Anticipation Multimedia Innovation (SAMI) Lab of France Telecom R&D Center (Beijing) in 2006. He worked as a senior engineer at the 28th research institute, CETC from 2007 to 2010. He worked as a visiting scholar at New Jersey Institute of Technology, NJ, USA from 2014 to 2015. His research interests include multimedia copyright protection, image forensics, image encryption and data authentication. He has published more than 30 papers, hosted and participated in more than 10 research projects.

[Xinpeng Zhang]: Dr Xinpeng Zhang has been with the faculty of the School of Communication and Information Engineering, Shanghai University since 2004, where he is currently a Professor. He is also with the faculty of the School of Computer Science, Fudan University. He received the BS degree in computational mathematics from Jilin University, China, in 1995, and the ME and PhD degrees in communication and information system from Shanghai University, China, in 2001 and 2004, respectively. He was with the State University of New York at Binghamton as a visiting scholar from January 2010 to January 2011, and Konstanz University as an experienced researcher sponsored by the Alexander von Humboldt Foundation from March 2011 to May 2012. He served IEEE Transactions on Information Forensics and Security as an Associate Editor from 2014 to 2017. His research interests include multimedia security, image processing, and digital forensics. He has published more than 200 papers in these areas.

Chuan Qin
Professor, School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China
qi@usst.edu.cn

Zhenxing Qian
Professor, School of Computer Science, Fudan University, Shanghai 200433, China
zxqian@fudan.edu.cn

Jinwei Wang
Professor, School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, Jiangsu, China
wjwei@nuist.edu.cn

Xinpeng Zhang
Professor, School of Computer Science, Fudan University, Shanghai 200433, China
zhangxinpeng@fudan.edu.cn