Multimedia Security: Novel Steganography and Privacy Preserving

Zhenxing Qian, Kim-Kwang Raymond Choo, Rémi Cogranne, Xinpeng Zhang

Hindawi
Security and Communication Networks
Volume 2018, Article ID 6390945, 2 pages
https://doi.org/10.1155/2018/6390945

Editorial

Multimedia Security: Novel Steganography and Privacy Preserving

Zhenxing Qian,[1] **Kim-Kwang Raymond Choo**,[2] **Rémi Cogranne**,[3] **and Xinpeng Zhang**[4]

[1]*Shanghai Institute for Advanced Communication and Data Science, School of Communication and Information Engineering, Shanghai University, Shanghai, China*
[2]*Department of Information Systems and Cyber Security, University of Texas, San Antonio, San Antonio, TX 78249, USA*
[3]*Laboratory of Systems Modeling and Dependability, Systems, Networks & Telecommunications, Troyes University of Technology, Troyes, France*
[4]*Shanghai Institute of Intelligent Electronics & Systems, School of Computer Science, Fudan University, Shanghai, China*

Correspondence should be addressed to Zhenxing Qian; zxqian@shu.edu.cn

Received 26 August 2018; Accepted 26 August 2018; Published 9 September 2018

Multimedia security is not a new research topic, as there have been a large body of work on various aspects of multimedia security. However, there remain a number of open research challenges, partly due to advances in multimedia and other related consumer technologies, for example, threats to conventional steganography due to emerging machine/deep learning-based steganalysis approaches. Thus, there is a need to design steganography approaches to mitigate such steganalysis efforts. Another ongoing challenge is how to ensure the privacy of multimedia data and the processing of such data, given constant advances in computational capabilities and big data analytics.

In this special issue, we aim to provide readers with a broad overview of multimedia security, such as novel steganography, privacy preserving on cloud computing, and multimedia tampering detection.

To achieve covert transmission, one could implement steganography in a cover. G. Swain (in "High Capacity Image Steganography using Modified LSB Substitution and PVD against Pixel Difference Histogram Analysis") demonstrated how we can expand the embedding capacity while mitigating steganalysis efforts. Another article on steganography was presented by J. He et al. ("A Novel AMR-WB Speech Steganography Based on Diameter-Neighbor Codebook Partition"). The authors used speech signals as covers to realize covert transmissions.

In addition to the use of covers, other approaches such as those based on images and audios can also be used to transmit secret data. For example, P. Cao et al. (in "A Wireless Covert Channel Based on Constellation Shaping Modulation") developed a system to transmit secret data over wireless channels, based on constellation shaping modulation. With constant advances in steganography solutions, X. ShuangKui et al. (in "A Modification-Free Steganography Method Based on Image Information Entropy") investigated the possibility of transmitting secret data in big data. Since secret data are directly mapped to the entropies of the covers, no modification is required when transmitting a single cover. For steganography, D. Hu et al. (in "Adaptive Steganalysis Based on Selection Region and Combined Convolutional Neural Networks") explained how to mitigate adaptive steganography by analyzing the selected regions of the covers using deep learning.

In terms of privacy preservation, a number of articles in this special issue focused on achieving privacy in the cloud computing environment. For example, during outsourcing of computations task from the user(s) to the cloud, Y. Ren et al. (in "Noninteractive Verifiable Outsourcing Algorithm for Bilinear Pairing with Improved Checkability") and H. Zhu et al. (in "Outsourcing Set Intersection Computation Based on Bloom Filter for Privacy Preservation in Multimedia Processing") presented two outsourcing protocols for bilinear

pairing and set intersection computations, respectively. The authors claimed that both protocols were more efficient and secure than prior work.

Multimedia indexing in encrypted domain is also another popular topic in privacy preservation. Hence, H. Liang et al. (in "Secure and Efficient Image Retrieval over Encrypted Cloud Data") proposed an efficient ciphertext retrieval algorithm, using balanced index tree and partial encryption. On the topic of labeling encrypted data in the cloud, D. Xu et al. (in "Separable Reversible Data Hiding in Encrypted Images Based on Two-Dimensional Histogram Modification") and X. Chen et al. (in "Improved Encrypted-Signals-Based Reversible Data Hiding Using Code Division Multiplexing and Value Expansion") proposed two reversible data hiding protocols for encrypted images, respectively. The use of watermarking to protect user privacy in the cloud environment was demonstrated by K. Liu et al. (in "A Cloud-User Protocol Based on Ciphertext Watermarking Technology").

In this special issue, multimedia forensics and network security were also discussed. For example, Y. Sun et al. (in "Nonoverlapping Blocks Based Copy-Move Forgery Detection"), H. Wang et al. (in "Perceptual Hashing-Based Image Copy-Move Forgery Detection"), and D. Niu et al. (in "Reference Sharing Mechanism-based Self-embedding Watermarking Scheme with Deterministic Content Reconstruction"), respectively, studied passive forensics, copy-move forgery detection, and watermarking. On the topics of network attack, R. Zhang et al. in ("Constructing APT Attack Scenarios Based on Intrusion Kill Chain and Fuzzy Clustering") presented an approach to simulate advanced persistent threat (APT) attack scenarios, and J. Chen (in "A Survey on Breaking Technique of Text-based CAPTCHA") surveyed existing approaches to circumventing CAPTCHA.

In conclusion, while the breadth and depth of the articles in this issue have contributed to the knowledge gap in multimedia security, many other challenges remain. It is hoped that the advances reported in this special issue will inspire new areas of research in the near future.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Zhenxing Qian
Kim-Kwang Raymond Choo
Rémi Cogranne
Xinpeng Zhang