Machine Learning for Wireless Multimedia Data Security

Pan, Zhaoqing; Yang, Ching-Nung; Sheng, Victor S.; Xiong, Naixue; Meng, Weizhi

Published in:
Security and Communication Networks

Link to article, DOI:
10.1155/2019/7682306

Publication date:
2019

Document Version
Publisher’s PDF, also known as Version of record

Link back to DTU Orbit

Citation (APA):
Pan, Z., Yang, C.-N., Sheng, V. S., Xiong, N., & Meng, W. (2019). Machine Learning for Wireless Multimedia Data Security. Security and Communication Networks, 2019, [7682306]. https://doi.org/10.1155/2019/7682306
Machine Learning for Wireless Multimedia Data Security

Zhaoqing Pan,1 Ching-Nung Yang,2 Victor S. Sheng,3 Naixue Xiong,4 and Weizhi Meng5

1 School of Computer and Software, Jiangsu Engineering Center of Network Monitoring and Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, Nanjing University of Information Science and Technology, Nanjing, China
2 Department of Computer Science and Information Engineering, National Dong Hwa University, Hualien, Taiwan
3 Department of Computer Science, University of Central Arkansas, Conway, AR, USA
4 College of Intelligence and Computing, Tianjin University, Tianjin, China
5 Department of Applied Mathematics and Computer Science, Technical University of Denmark, Kongens Lyngby, Denmark

Correspondence should be addressed to Zhaoqing Pan; zhaoqingpan@nuist.edu.cn

Received 17 March 2019; Accepted 17 March 2019; Published 1 April 2019

Copyright © 2019 Zhaoqing Pan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the rapid development of multimedia technologies, the collection and modification of wireless multimedia data have become greatly convenient and easy. Meanwhile, the wireless multimedia data also made sensitive information available to potential attackers. The credibility of digital wireless multimedia data has thus decreased if the wireless multimedia data cannot be well protected. In addition, the copyright and privacy of wireless multimedia data also are easy to be infringed. Particularly, the data storage and computation have to be delegated to the powerful but always untrusted cloud, which has led to a series of challenging security and privacy threats.

Nowadays, artificial intelligence (AI) technology has been widely used in academia and industry. Machine learning can be regarded as one of the most important AI technologies, and it has been successfully used in image processing, pattern recognition, computer vision, natural language processing, and so on. Currently, the traditional steganography and security of encrypted wireless multimedia data face a lot of challenges. Thus, new types of steganography and encryption of wireless multimedia data, including audio, image, and video, are urgently needed to explore. Moreover, in new environments like cloud computing, the distribution and processing of wireless multimedia data also face more new challenges. For example, how to securely process wireless multimedia data in cloud computing to preserve the privacy of wireless multimedia data and how to reliably solve multiparty computing by outsourcing are still open questions.

This special issue aims to address the wireless multimedia data security problems by using machine learning methods. It includes seventeen papers, and the details of each paper are introduced one by one as follows.

To address the security problem of the multimedia data of the Internet of Thing (IOT), E. Min et al. proposed an intrusion detection system, which is based on the statistical and payload features. To extract the useful information from the payloads, the word embedding and text-convolutional neural network are used. Then, the random forest algorithm is applied to the final classification. Experimental results show that the proposed algorithms achieve better performance than the state-of-the-art algorithms.

To address the security problem of online transaction, Z. Zhang et al. proposed an online transaction fraud detection method based on the convolutional neural network (CNN). Since the low-dimensional and nonderivative online transaction data are used as the network input, the proposed method obtains an outstanding performance compared to the existing CNN-based fraud detection methods.

To address the limitations of the traditional encrypting algorithms, G. Xin et al. proposed an adaptive audio steganography algorithm. The proposed algorithm is based on the interval and variable low bit coding. Experimental
results show that the proposed algorithm achieves a better performance in embedding rate and invisibility than the other state-of-the-art audio steganography algorithms.

H. Dai et al. proposed privacy-preserving sorting algorithms for clouds, which are based on the basis of the logistic map. The security analysis and experimental results demonstrate that the proposed algorithms can well protect data privacy and provide efficient sorting on encrypted data.

Y. Zheng et al. proposed an improved image deep learning hash algorithm to learn the compact binary codes for image search. The proposed algorithm includes three parts, the feature extraction, deep secondary search, and image classification, respectively. Experimental results show that the proposed algorithm can efficiently identify the illegal images.

To address the security problems of lightweight block ciphers, P. Zhang and W. Zhang proposed a mixed-integer linear programming method to verify the security of Skinny-64/192. Experimental results show that the proposed method can significantly reduce the number of variables and improve the running speed of the computer.

For intrusion detection, Y. Xue et al. proposed an evolutionary computation based feature selection algorithm, in which the self-adaptive differential evolution is adopted. Experimental results show that the proposed algorithm is more promising than the state-of-the-art algorithms.

Based on the ensemble learning, Z. Zhang et al. proposed a wireless multimedia device identification system. The proposed system includes three parts, signal detection, RFF extraction, and classification model, respectively. Experimental results show that the identification rate of the proposed method can reach over 95%.

To deal with the data encryption problem, C. Ge et al. proposed a new source hiding identity-based proxy re-encryption method (SHIB-PRE). The proposed SHIB-PRE method supports a proxy to convert a user’s encrypted data to a new user’s ciphertext when the proxy has the proxy reencryption key.

To deal with the security problem of the wireless network, L. Fang et al. proposed a fuzzy-conditional proxy broadcast reencryption method, in which the proxy uses a broadcast reencryption key to reencrypt the encrypted wireless multimedia data. The comparison results show that the proposed method can well address the security problems.

To protect the security of Android applications, S. Niu et al. proposed an improved permission management method, which is based on the machine learning algorithm. The proposed method uses a dynamic permission management database, and only the permission in the database can be used in this application. Experimental results show that the proposed method efficiently increases the flexibility of permission management.

To address the accuracy problem of single biometric method, Z. Wu et al. proposed a multimodal fusion algorithm for fingerprint and voiceprint, which is based on a dynamic Bayesian. Experimental results show that the proposed algorithm can efficiently improve the recognition rate and stability.

To deal with the problem of plaintext attack, X. Hu and Y. Zhao adopted the backpropagation neural networks to perform cryptanalysis on the Advanced Encryption Standard (AES). Experimental results show that the proposed algorithm can efficiently restore the entire byte.

To improve the image quality, C. Li et al. proposed a single image deraining algorithm by using the generative adversarial networks. Experimental results show that the proposed algorithm achieves an excellent performance in terms of image quality and computing efficiency.

L. Tan et al. proposed a visual secret sharing method for quick response (QR) code, which uses the grayscale QR codes as cover images and the binary QR code as the secret image. Experimental results show that the proposed method is robust to images with various types of distortions.

To deal with security problem of multimedia data in cloud, X. Zhao et al. proposed a hybrid homomorphic plaintext slot-wise switching algorithm; it can efficiently reduce computing and storage complexities of bootstrapping key generation. Experimental results show that the proposed algorithm can significantly optimize the bootstrapping procedure.

To address the security problem of medical image, B. Ma et al. proposed a reversible data hiding algorithm by using code division multiplexing and machine learning techniques. Experimental results prove that the proposed algorithm achieves outstanding performance in terms of data embedding capacity.

Conflicts of Interest

The editors declare that they have no conflicts of interest regarding the publication of this special issue.

Acknowledgments

We would like to thank all of the authors who have submitted their work to this special issue. We also gratefully thank anonymous reviewers for providing helpful suggestions to improve the quality of the submissions. The launch of this special issue was supported in part by the National Natural Science Foundation of China under Grant no. 61501246, in part by the National Science Foundation of Jiangsu Province of China under Grant no. BK20150930, in part by the Six Talent Peaks Project of Jiangsu Province under Grant no. XYDXXJS-04, in part by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology, and in part by the Project through the Priority Academic Program Development of Jiangsu Higher Education Institutions.

Zhaoqing Pan
Ching-Nung Yang
Victor S. Sheng
Naixue Xiong
Weizhi Meng
