Multimedia Systems (2021) 27:301–302
https://doi.org/10.1007/s00530-021-00809-2

EDITORIAL

Special issue on low complexity methods for multimedia security

Guorui Feng[1] · Sheng Li[2] · Haoliang Li[3] · Shujun Li[4]

Received: 5 May 2021 / Accepted: 7 May 2021 / Published online: 18 May 2021

Nowadays, more and more mobile devices are being used in our daily life. A vast amount of multimedia data, including audios, images and videos, are produced by the mobile devices every single second. These data are usually stored in a networked environment for people to view, share, or comment. As such, people's locations, status, or live actions can be seen, traced or monitored. The shared multimedia data are also under the risk of being illegally used or manipulated. The research of multimedia security is to prevent or detect the criminal activities related to multimedia data, including multimedia authentication, multimedia content security, multimedia privacy security, etc. These fields can be detailed as privacy protection, information hiding and detection, digital forensics, secure processing, etc. To process the huge amount of multimedia data, one important issue is to reduce the burden of the servers effectively. On possible solution is to take advantage of the computational power of the mobile devices. However, the computational power of the mobile devices is usually limited, and it is necessary to develop relevant algorithms that are with low computational complexity. In the past few years, researchers have developed a great number of schemes for multimedia security. However, relatively few techniques are applicable on the mobile devices.

This special issue aims at promoting the research on low complexity methods for multimedia security, which includes lightweight learning and modeling for multimedia data forensics and anti-forensics, low complexity multimedia privacy protection schemes, low complexity data hiding schemes, and the attacks and counter measures for the authenticity of multimedia data. In total, this special issue attracts 26 high quality submissions, where each of the submission is peer reviewed with at least two reviewers. After rigorous review process, we accept ten submissions with an acceptance rate of 38.5%. The accepted papers fall into the following three research areas, including multimedia data hiding and steganography, multimedia forensics and steganalysis, and multimedia hashing and retrieval.

1 Multimedia data hiding and steganography

The paper entitled "Reversible data hiding in encrypted medical DICOM image", co-authored by Ping Kong, Di Fu, Xinran Li and Chuan Qin, proposes a novel reversible data hiding scheme in encrypted domain for medical DICOM images. This scheme segments the DICOM image and conducts the data embedding into a partial of the encrypted version. The redundancy of the pixel cells in the DICOM images is utilized to accommodate some auxiliary data for image recovery, which helps to accurately detect the tampered area on the receiver side.

The paper entitled "Low complexity reversible data hiding in encrypted image via MSB hierarchical coding and LSB compression", co-authored by Fang Cao, Xiaokang Qian and Bowen An, proposes a low-complexity reversible data hiding scheme for encrypted images based on MSB hierarchical coding and LSB compression. This scheme encrypts the original image using pixel encrypting, block and pixel scrambling. The MSBs of the image blocks are hierarchical encoded and the LSBs are compressed to make room for data embedding. Experimental results demonstrate the advantage of this scheme in terms of rate-distortion performance.

The paper entitled "Steganography in animated emoji using self-reference", co-authored by Zhiying Zhu, Qichao Ying, Zhenxing Qian and Xinpeng Zhang, proposes an interesting steganographic scheme for animated emoji. In this scheme, a self-reference algorithm is proposed to improve the security of steganography, where the relations between adjacent frames of the cover emoji are considered to construct the distortion function for syndrome trellis coding

✉ Guorui Feng
grfeng@shu.edu.cn

[1] Shanghai University, Shanghai, China

[2] Fudan University, Shanghai, China

[3] Nanyang Technological University, Singapore, Singapore

[4] University of Kent, Canterbury, UK

(STC) based data embedding. Experimental results show that this method offers better performance than the state-of-the-art works in terms of security.

The paper entitled "Audio steganography with less modification to the optimal matching CNV-QIM path with the minimal Hamming distance expected value to a Secret", co-authored by Xinhao Sun, Kaixi Wang and Shujun Li, proposes a novel audio steganographic scheme by taking advantage of complementary neighbor vertex (CNV), where the parameter sequence with the minimal hamming distance expected value (HDEV) is selected for data embedding. The experimental results demonstrate the advantage of the proposed scheme in terms of preserving audio quality.

2 Multimedia forensics and steganalysis

The paper entitled "Low complexity fake face detection based on forensic similarity", co-authored by Zhaoguang Pan, Yanli Ren and Xinpeng Zhang, proposes a low complexity fake face detection scheme by exploring the consistency between the face area and background area, which is performed by a similarity measure to determine the authenticity of the face video frames. This method is shown to be better than the Xception with over 8% performance gain in accuracy on Celeb-DF data set and lower computational complexity.

The paper entitled "Resampling parameter estimation via dual-filtering-based convolutional neural network", co-authored by Lin Peng, Xin Liao and Mingliang Chen, proposes an image resampling parameter estimation scheme based on a dual-filtering based convolutional neural network (CNN), where two parallel high-pass filters are deployed on the CNN architecture to enhance the resampling traces. This scheme is shown to be better than the state-of-the-art methods for image resampling parameter estimation.

The paper entitled "Low complexity JPEG steganalysis via filters optimization from symmetric property", co-authored by Weiwei Luo, Jianwu Dang, Wenrun Wang and Fengwen Zhai, proposes a low complexity JPEG steganalysis scheme by selecting proper filters to capture the discriminative features from the subtle embedding traces. This scheme is shown to be able to improve the detection performance of JPPE steganalysis with a low feature dimension.

The paper entitled "Steganalysis of convolutional neural network based on neural architecture search", co-authored by Hongbo Wang, Xingyu Pan, Lingyan Fan and Shuofeng Zhao, proposes a neural architecture search (NAS) algorithm for image steganalysis, where a long-span residual structure is added to the residual network to boost the performance. This method is shown to be effective for detecting the stego-images generated by different steganographic schemes with various payloads.

3 Multimedia hashing and retrieval

The paper entitled "Robust and fast image hashing with two-dimensional PCA", co-authored by Xiaoping Liang, Zhenjun Tang, Xiaolan Xie, Jingli Wu and Xianquan Zhang, proposes a robust and fast image hashing based on two-dimensional (2D) principal component analysis (PCA) and saliency map. The saliency map is computed by a luminance contrast attention model and the use of 2D PCA helps to learn a compact and discriminative code for fast image hashing. This scheme is shown to be better than the state-of-the-art in both the classification accuracy and speed.

The paper entitled "A privacy-preserving and traitor tracking content-based image retrieval scheme in cloud computing", co-authored by Zhangdong Wang, Jiaohua Qin, Xuyu Xiang and Yun Tan, proposes a content-based image retrieval scheme which is able to preserve the privacy of image content and track the traitors. This scheme incorporates DenseNet for feature extract, and a one-way hash function to protect copyright and user information. A reversible information hiding algorithm is also adopted for traitor tracking. Experimental results demonstrate the advantage of this scheme for privacy-preserved image retrieval as well as the ability for traitor tracking.