Guest Editorial: Information Hiding and Forensics for Multimedia Security

Chuan Qin¹ · Dengpan Ye² · Xiangyang Luo³

Published online: 31 August 2016

© Springer Science+Business Media New York 2016

Nowadays, information hiding techniques, including watermarking, steganography, and steganalysis, have been the efficient and important applications for covert communication. For a country or organization, information hiding techniques can be utilized to transmit confidential messages using steganographic techniques, protect copyright of a software or digital publication using watermarking techniques, etc. However, above techniques may also be used by the terrorists or illegal guys to endanger national security and destroy social stabilization. Therefore, steganalysis as the inverse technique is also required for further research. In addition, multimedia forensic that can authenticate multimedia data in a blind way has been widely studied in recent years, and many digital forensic techniques have been proposed by using the methods in the areas such as machine learning, signal and image processing, and communications. Nevertheless, there are some notable shortcomings in research methodologies that still need improvements.

This special issue aims to bring together researchers in the related fields of information hiding and digital forensic that can be utilized for multimedia security, and it demonstrates pioneer works, investigates novel solutions, and discusses future trends in these fields. According to the rigorous review process that consisted of several rounds, each submission to the special issue was rigorously reviewed by at least three anonymous experts. Finally, 28 papers are selected to be included in this special issue, which fall into eight main categories: (1)

✉ Chuan Qin
qin@usst.edu.cn

Dengpan Ye
yedp@whu.edu.cn

Xiangyang Luo
xiangyangluo@126.com

¹ School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China

² School of Computer, Wuhan University, Wuhan 430072, China

³ Zhengzhou Information Science and Technology Institute, Zhengzhou 450001, China

digital watermarking, (2) *steganography*, (3) *steganalysis*, (4) *reversible data hiding*, (5) *signal processing in encrypted domain*, (6) *digital forensics*, (7) *visual cryptography and secret image sharing*, and (8) *other emerging techniques*. In the following, we discuss these papers briefly.

1. Digital watermarking

The paper titled “A Dual Fragile Watermarking Scheme for Speech Authentication” ([10.1007/s11042-015-2801-4](#)), co-authored by Qing Qian, Hong-Xia Wang, Yi Hu, Lin-Na Zhou, and Jin-Feng Li, proposes a hash-based dual fragile watermarking algorithm to achieve integrity authentication of speech files. In the proposed algorithm, two fragile watermarks are generated by using the transformed speech signal and MD5 hash function. During tampering detection, the extracted and the reconstructed watermarks are applied to construct two verification vectors and form a verification grid for the determination of modification type. Experimental results show that the proposed scheme has good performances of imperceptibility and fragility and the satisfactory capability of tampering localization and identification.

“Structure Compliant Local Warping of Images with Applications to Watermarking Attack” ([10.1007/s11042-015-2831-y](#)) is presented by Bin Yan, Xiao-Feng Liu, and Hong-Mei Yang. The authors study the localized geometric warping of images, which is known to be one of the most effective attacks on image watermarking systems. In this work, a multi-scale directional smoothing framework is proposed, in which local displacement vectors constrained by a multi-scale pyramid are smoothed with locally adaptive directional kernels. The test of attacking effects on two typical watermarking systems demonstrates that this approach does not degrade the attacking effects for Markov random field generated displacement field.

In another paper titled “Improved Logarithmic Spread Transform Dither Modulation Using a Robust Perceptual model” ([10.1007/s11042-015-2853-5](#)), Wenbo Wan, Ju Liu, Jiande Sun, and Di Gao propose an improved logarithmic spread transform dither modulation (STDM) watermarking method using a best-matched DCT-based perceptual JND model, which can keep insensitive to the changes caused by watermark embedding and attacks. Experimental results show that the proposed method is more robust than the existing JND model-based watermarking algorithms with the uniform fidelity and has a superior performance compared with the former perceptual STDM methods.

2. Steganography

The paper titled “Motion Vector-based Video Steganography with Preserved Local Optimality” ([10.1007/s11042-015-2743-x](#)), co-authored by Hong Zhang, Yun Cao, and Xianfeng Zhao, proposes a new video steganographic method to guarantee the local optimality of modified motion vectors. The method designates a search area that consists of candidate motion vectors and evaluates the local optimality of each motion vector in the search area. The one contributing the least to video compression efficiency degradation is chosen as the modified motion vector. Experimental results demonstrate that video steganography based on the proposed method is capable of resisting current best steganalysis while keeping the video compression performance.

Another paper titled “YouSkyde: Information Hiding for Skype Video Traffic” ([10.1007/s11042-015-2740-0](#)), co-authored by Wojciech Mazurczyk, Maciej Karaś, Krzysztof Szczypiorski, and Artur Janicki, proposes a new information hiding method

called as YouSkyde for Skype-based video conference calls. A YouSkyde proof-of-concept implementation is conducted detailedly in this paper. Experimental evaluation results demonstrate that the proposed method not only can provide a steganographic bandwidth as high as 0.93 kbps but also introduces negligible distortions into transmission quality with high undetectability.

In the paper “Adaptive Pixel Value Differencing Steganography Using both Vertical and Horizontal Edges” ([10.1007/s11042-015-2937-2](#)), Gandharba Swain proposes two pixel value differencing (PVD) steganographic schemes using adaptive ranges to improve the security. In the first scheme, for each 2×2 block, the left-upper and bottom-right corner pixels are targeted based on their correlation with the other two pixels. In the second scheme, for each 3×3 block, the central pixel is targeted for embedding. Both horizontal and vertical edges are considered in two schemes. The first scheme provides higher hiding capacity and the second scheme provides higher PSNR value.

3. Steganalysis

The paper titled “Steganalysis of HUGO Steganography Based on Parameter Recognition of Syndrome-Trellis-Codes” ([10.1007/s11042-015-2759-2](#)), co-authored by Xiangyang Luo, Xiaofeng Song, Xiaolong Li, Weiming Zhang, Jicang Lu, Chunfang Yang, and Fenlin Liu, analyzes the security of Highly Undetectable steGO (HUGO) steganography and proposes a corresponding steganalysis method. By using blind coding parameter recognition, the submatrix parameter of syndrome-trellis codes (STCs) is recognized correctly, and the message embedded by HUGO can be extracted correctly by decode algorithm of STCs. A number of experimental results show that the proposed steganalysis method can not only detect the stego-images reliably but also extract the embedded message correctly, which validates the existence of security flaw of HUGO steganography.

Another paper titled “Joint-Channel Modeling to Attack QIM Steganography” ([10.1007/s11042-015-3006-6](#)), co-authored by Hafiz Malik, K. P. Subbalakshmi, and R. Chandramouli, proposes a statistical steganalysis framework to attack quantization index modulation (QIM)-based steganography. The proposed method exploits that the quantization without data embedding decreases local randomness in the resulting quantized image. A parametric model is developed in this paper to characterize the channel-dependent local-randomness, and the maximum likelihood estimation (MLE) framework is used to estimate distribution parameters of the local-randomness mask. To improve detection accuracy, decisions from both detectors are fused to generate the final stego-detection decision. Experimental results show that this scheme can successfully detect QIM-stego images with very low false rates.

The paper titled “Spatial Steganalysis Using Redistributed Residuals and Diverse Ensemble Classifier” ([10.1007/s11042-015-2742-y](#)), co-authored by Jiang Yu, Xinpeng Zhang, and Fengyong Li, proposes a spatial steganalytic scheme by redistributed residuals and diverse ensemble classifier. In their scheme, the residuals obtained by local pixel predictors are shifted and suppressed to produce the redistributed residuals, and the 2929 dimension features are calculated from the first-order statistic of original and redistributed residuals, which can preserve long-range dependencies between pixels, especially for highly adaptive steganography. Compared with the reported schemes, the proposed scheme is effective at low embedding rate and is characterized by lower computational complexity.

In the paper titled “Stego Anomaly Detection in Images exploiting the Curvelet Higher Order Statistics using Evolutionary Support Vector Machine” ([10.1007/s11042-015-2984-8](#)),

S. Muthuramalingam, N. Karthikeyan, S. Geetha, and Siva S. Sivatha Sindhu present a new steganalyser by selecting the Curvelet sub-band image representation that can offer good discrimination ability of detecting stego anomalies in images. Also, the evolutionary-SVM model that provides promising classification rate is used to realize the system. An extensive empirical evaluation on a database including 5600 original and stego-images shows that the proposed scheme can outperform other previous steganalytic schemes.

4. Reversible data hiding

The paper titled “Improving Visual Quality of Reversible Data Hiding by Twice Sorting” ([10.1007/s11042-015-2824-x](https://doi.org/10.1007/s11042-015-2824-x)), co-authored by Yang Yang, Weiming Zhang, Xiaocheng Hu, and Nenghai Yu, proposes a twice sorting scheme to achieve reversible data hiding in digital images. In the proposed scheme, image pixels are sorted and divided into several levels by a smoothness criterion and then sorted twice with just noticeable difference (JND) in each level. Secret bits are embedded into the predicted errors of pixels in the sorted order. Experimental results show that this method can outperform previous JND-related RDH schemes on not only PSNR but also other visual quality indices, such as structural similarity (SSIM) and JND.

In the paper titled “Block-Based Reversible Data Hiding with Multi-Round Estimation and Difference Alteration” ([10.1007/s11042-015-2825-9](https://doi.org/10.1007/s11042-015-2825-9)), Yueh-Hong Chen, Hsiang-Cheh Huang, and Chuan-Chang Lin propose a reversible data hiding algorithm based on the alteration of difference values relating to original image. In this algorithm, they employ the block-based, multi-round prediction to improve the performances. Simulation results demonstrate that the proposed algorithm achieves the enhanced amount of capacity and better image quality, which also has the advantage of its easy implementation for medical applications.

Another paper titled “A Reversible Steganographic Scheme for VQ Indices Based on Joint Neighboring and Predictive Coding” ([10.1007/s11042-015-2828-6](https://doi.org/10.1007/s11042-015-2828-6)), co-authored by The Duc Kieu and Andrew Rudder, presents a reversible steganographic method to embed secret data into the vector quantization (VQ) compressed images. The method based on joint neighboring and predictive coding uses left and upper neighboring VQ indices and the difference between the current VQ index and the predicted value to achieve a low bit-rate. Experimental results show that this method obtains embedding rates of 1, 2, 3, and 4 bits per index with respective average bit rates of 0.409, 0.471, 0.534, and 0.596 bit per pixel for a 256-sized codebook.

Nowadays, a large amount of electrocardiography (ECG) signals as well as patient confidential information are transmitted on the Internet. In the paper titled “Protecting Patient Confidential Information Based on ECG Reversible Data Hiding” ([10.1007/s11042-015-2706-2](https://doi.org/10.1007/s11042-015-2706-2)), Hui Wang, Weiming Zhang, and Nenghai Yu propose a method to embed patient confidential data into ECG signal reversibly, while keeping its high visual quality. The authors also propose a unified embedding-scrambling method to guarantee the security of patient privacy as well as the ECG signal itself. Experimental results demonstrate that both of the proposed methods are reversible, and the latter method can achieve high embedding payload.

5. Signal processing in encrypted domain

In the paper titled “Block Cipher Based Separable Reversible Data Hiding in Encrypted Images” ([10.1007/s11042-015-2760-9](https://doi.org/10.1007/s11042-015-2760-9)), Zhenxing Qian, Xinpeng Zhang, Yanli Ren, and Guorui Feng conduct the study on reversible data hiding in encrypted images (RDH-EI), and they aim to present an alternative method feasible to block-enciphered images rather than stream-enciphered images. In this method, the server

embeds additional bits into encrypted image with an embedding key to generate the marked encrypted image. On the receiver side, data extraction, image decryption, and image recovery can be implemented in a separable way. Compared with the existing block cipher-based RDH-EI method, the proposed method can achieve satisfactory hiding capacity.

The paper titled “Lossless Data Hiding Algorithm for Encrypted Images with High Capacity” ([10.1007/s11042-015-2920-y](https://doi.org/10.1007/s11042-015-2920-y)), co-authored by Shuli Zheng, Dandan Li, Donghui Hu, Dengpan Ye, Lina Wang, and Jinwei Wang, proposes another reversible data hiding algorithm for encrypted images. In this algorithm, the LSBs of encrypted image are losslessly compressed to leave place for secret data. With auxiliary bit stream, lossless compression is realized by the Hamming distance calculation between the LSB stream and auxiliary stream. Experiments show the feasibility and efficiency of the proposed algorithm, especially for hiding capacity, decrypted image quality, and error-free recovery with increasing payload.

In the paper titled “High-capacity Separable Data Hiding in Encrypted Image Based on Compressive Sensing” ([10.1007/s11042-015-2922-9](https://doi.org/10.1007/s11042-015-2922-9)), Di Xiao, Hongkun Cai, Yong Wang, and Sen Bai propose a new scheme for high-capacity separable data hiding in encrypted images using compressive sensing. Different encryption methods are applied on the DC and AC coefficient matrices, and secret bits are hidden in the reserved room of encrypted image to produce the encrypted image with embedded data by compressive sensing. The way to obtain image content or/and additional data is separable according to the keys that the receiver owns. Experimental results show that this scheme has the superiorities of high capacity, anti-packet loss, and cipher text compressibility.

The paper titled “AC-Coefficient Histogram-Based Retrieval for Encrypted JPEG Images” ([10.1007/s11042-015-2741-z](https://doi.org/10.1007/s11042-015-2741-z)), co-authored by Hang Cheng, Xinpeng Zhang, and Jiang Yu, proposes a new retrieval scheme for encrypted JPEG images. In this scheme, the DC and AC coefficients of JPEG images are encrypted and transmitted to the server that can provide retrieval service. When receiving an encrypted query image, the server with no knowledge of plaintext content can obtain its AC-coefficient histogram. By calculating the distances between the histograms of encrypted query image and database image, the server can output the encrypted images closest to the query image to the authorized user.

In another paper titled “Encryption Domain Content-based Image Retrieval and Convolution through a Block-based Transformation Algorithm” ([10.1007/s11042-015-2917-6](https://doi.org/10.1007/s11042-015-2917-6)), Jia-Kai Chou, Chuan-Kai Yang, and Hsing-Ching Chang propose a block-based transformation algorithm to achieve image content protection. Under the content protection framework, image retrieval and image convolution can also be realized. Security analyses are conducted to prove that the proposed image encryption scheme achieves the security in both statistical and computational aspects. Experimental results demonstrate the decent performance of the proposed encryption domain image retrieval and convolution with acceptable storage overhead.

6. Digital forensics

The paper titled “Forensics and Counter Anti-forensics of Video Inter-frame Forgery” ([10.1007/s11042-015-2762-7](https://doi.org/10.1007/s11042-015-2762-7)), co-authored by Xiangui Kang, Jingxian Liu, Hongmei Liu, and Z. Jane Wang, studies the forensic and anti-forensic techniques for video inter-frame forgery. The authors first improve an existing

video frame deletion detection algorithm, and the improvement lies in the combination of two properties resulted from video frame deletion, the periodicity and the magnitude of the fingerprint in the P-frame prediction error. A counter anti-forensic approach by estimating the true prediction error and comparing it with the prediction error stored in videos is also proposed in this paper. Experimental results show that the proposed forensic and counter anti-forensic methods not only outperform existing methods in detecting frame deletion and anti-forensics but also outperform them in the VIF game.

In another paper titled “Detection of Double MP3 Compression Based on Difference of Calibration Histogram” ([10.1007/s11042-015-2758-3](#)), Yanzhen Ren, Mengdi Fan, Dengpan Ye, Jing Yang, and Lina Wang propose a new method to detect the presence of double MP3 compression, which is based on the difference of calibration histogram (DCH) characteristic. The features in this method are extracted from the difference of the statistics of MDCT coefficients between test audio and its calibrated audio. The proposed method can also be utilized to estimate the bit-rate of the first-time MP3 encoding from recompressed MP3 files. Experimental results demonstrate that the features used in the proposed method are sensitive to double MP3 compression and achieve higher accuracy than those of existing methods, especially for the same-transcoded and down-transcoded MP3 recompression.

The paper titled “Rebuilding the Credibility of Sensor-based Camera Source Identification” ([10.1007/s11042-015-3072-9](#)), authored by Hui Zeng, studies the problem of camera source identification (CSI). In order to rebuild the credibility of the CSI method, a simple and effective countermeasure based on noise level estimation is proposed in this paper, which can be considered as a suitable patch on the traditional CSI methods due to the low complexity. Experimental results show the proposed method has the capability of capturing the traces left by the anti-forensic methods.

7. Visual cryptography and secret image sharing

The paper titled “General Construction for XOR-based Visual Cryptography and Its Extended Capability” ([10.1007/s11042-016-3250-4](#)), co-authored by Hao Hu, Gang Shen, Zhengxin Fu, Bin Yu, and Jingjing Wang, focuses on strong access structures and presents a general construction of visual cryptography scheme with XOR (VCSXOR), which can provide flexible sharing strategies and perfect reconstruction of secret image. The authors also propose a new region incrementing VCS based on XOR (RIVCSXOR). Experimental results demonstrate that the proposed schemes can enrich the application scenarios effectively and have better performances than some reported schemes.

In another paper titled “Secret Image Sharing with Smaller Shadow Sizes for General Access Structures” ([10.1007/s11042-015-2734-y](#)), Ying-Ru Chen, Ling-Hwei Chen, and Shyong Jian Shyu conduct the study on secret image sharing (SIS), and they propose three polynomial-based SIS schemes for general access structures (GAS). These schemes can reconstruct secret image perfectly without any extra-information. Some proof and analysis on the shadow sizes of the three schemes are presented for choosing the one with the smallest size. Superior performance of the proposed schemes compared with two existing schemes and the security issue are also tested and addressed.

The paper titled “Reversible Secret Image Sharing Scheme in Encrypted Images” ([10.1007/s11042-016-3844-x](#)), co-authored by Sang-Ho Shin and Ki-Hyun Jung, proposes a reversible secret image sharing scheme in encrypted images in order to protect the copyright and privacy of cover image. The polynomial arithmetic operation over $GF(2^8)$ is used during the sharing of encrypted shadow images, and the coefficient of the highest-order term is fixed to one in order to prevent the problem of overflow and security. In the reconstruction procedure, secret data can be extracted and cover image can be reconstructed reversibly from encrypted shadow images by Lagrange interpolation. Experimental results show that the PSNR value of shadow image with respect to encrypted image in this scheme is more than 44 dB, and the embedding capacity is 524,288 bits on average.

8. Other emerging techniques

The paper titled “A Secure Image Encryption Scheme Based on Chaotic Maps and Affine Transformation” ([10.1007/s11042-015-2973-y](#)), co-authored by Jawad Ahmad and Seong Oun Hwang, proposes an efficient chaos-based image encryption scheme with higher key space, which can achieve a significantly larger key space even with a single round of encryption. The proposed scheme removes correlation among image pixels via random chaotic sequences by XOR and addition operations, and the affine transformation is used to obtain the final ciphertext image that can resist against numerous attacks. The security of this scheme is demonstrated through the analysis of histogram, contrast, PSNR, entropy, correlation, key space, key sensitivity, and differential attack.

Another paper titled “Mobile Crowd-sensing Context Aware based Fine-grained Access Control Mode” ([10.1007/s11042-015-2693-3](#)), co-authored by Dengpan Ye, Yuan Mei, Yueyun Shang, Jixiang Zhu, and Kun Ouyang, proposes a context-aware model combined with crowd-sensing paradigm to achieve fine-grained measurement of user’s current context. In the scheme, the context is categorized by kinds of attributes, and the attribute-tree based context-aware access control model is presented to protect user’s privacy and confidential information. Experimental results show that the proposed model is fine-grained, efficient, and flexible to apply on different mobile platforms.

In the paper titled “A Novel Authorization Delegation Scheme for Multimedia Social Networks by Using Proxy Re-encryption” ([10.1007/s11042-015-2929-2](#)), Weining Feng, Zhiyong Zhang, Jian Wang, and Linqian Han propose a new authorization delegation scheme based on the proxy re-encryption mechanism, which enables one user to delegate digital rights to another or the group of users and achieves fine-grained authorization delegation. The proposed scheme can achieve the security share of multimedia content and the functionality of digital rights management with resolving the limited access control list.

The fulfillment of this special issue was achieved by pleasant collaboration. We wish to thank all the authors for submitting their excellent contributions and also appreciate the reviewers and the Springer staffs for their hard work. We do expect that the papers included in this special issue could make the audience of Multimedia Tools and Applications satisfied and interested. Specially, we would like to deeply thank Prof. Borko Furht, Editor-in-Chief of Multimedia Tools and Applications, for his great supports and helps from the beginning to the eventual publication of this special issue.

Chuan Qin The author received the B.S. degree in electronic engineering and the M.S. degree in signal and information processing from Hefei University of Technology, Anhui, China, in 2002 and 2005, respectively, and the Ph.D. degree in signal and information processing from Shanghai University, Shanghai, China, in 2008. Since 2008, he has been with the faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, where he is currently an Associate Professor. He was with Feng Chia University at Taiwan as a Postdoctoral Researcher and Adjunct Assistant Professor from July 2010 to July 2012. His research interests include digital image processing and multimedia security. He has published more than 70 papers in these research areas.

Dengpan Ye The author was born in Hubei, China. He received the B.A.Sc in automatic control from SCUT in 1996 and Ph.D. degree at NJUST in 2005, respectively. He worked as a Postdoctoral Fellow in Information System School of Singapore Management University. And since 2012, he has been a professor in the school of computer science at Wuhan University. His research interests include Machine Learning and multimedia security. He is the author or co-author of more than 30 refereed journal and conference papers.

Xiangyang Luo The author received the M.S. degree and the Ph.D. degree from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2004 and 2010, respectively. From 2006 to 2007, he was a visiting scholar of the Department of Computer Science and Technology of Tsinghua University. He is the author or co-author of more than 70 refereed international journal and conference papers. He is currently an associate professor and doctoral supervisor of the State Key Laboratory of Mathematical Engineering and Advanced Computing, and Zhengzhou Science and Technology Institute. He obtained the Nomination Award of 2012 China National Outstanding Doctoral Dissertation. In 2013, he obtained the Award of Outstanding Youth of Science and Technology Invitation of Henan Province of China. In 2015, he obtained the ACM China Zhengzhou Rising Star Award. His research interest includes multimedia security, image steganography, and steganalysis.