International Journal of Security and Its Applications
Vol. 10, No. 7 (2016) pp.93-102
http://dx.doi.org/10.14257/ijsia.2016.10.7.09

Parallel Joint Fingerprinting and Encryption for Social Multimedia Sharing Based on Game of Life

Conghuan Ye, Zenggang Xiong*, Yaoming Ding, Xuemin Zhang, Guangwei Wang, Fang Xu and Kaibing Zhang

School of Computer and Information Science, Hubei Engineering University, Xiaogan, China
E-mail:jkxxzg@163.com

Abstract

The advent of online social network and mobile multimedia communication has made content sharing in social network easier and more efficient. It is very important to combine fingerprinting and encryption for social multimedia content protection. In this paper, a parallel JFE (joint fingerprinting and encryption) framework is proposed. Firstly, the multi-level social fingerprint code is produced using social network analysis, and followed by TSH (tree structure harr) wavelet decomposition for multimedia content. And then, fingerprints are embedded into all the LL, HL and LH subbands parallelly. At last, GoL(Game of Life) are used to for confusion for wavelet coefficients parallelly. The proposed parallel JFE method, to the best of our knowledge, is the first JFE method using GoL in the TSH wavelet domain for security and privacy. Theory analysis and experimental results demonstrate the effectiveness of the proposed JFE scheme.

Keywords*: multimedia fingerprinting, multimedia encryption, social multimedia sharing, CA (Cellular automata), social network*

1. Introduction

The rapid development of online social network and mobile multimedia communication makes social multimedia content sharing in social network very easy, digital multimedia content sharing in social network has witnessed a phenomenal growth over the past decade. Social multimedia sharing offers new challenges for online social network such as privacy and security issues. In order to protect privacy, secure distribution and sharing social multimedia content in social network is becoming more and more important.

Multimedia security techniques, such as fingerprinting and encryption, sometimes need to be carried out for privacy protection. For example, the owner distribute multimedia content distribute to users with multilevel network [1]. Multimedia encryption is an effective way to protect the original multimedia content [2]. Full encryption can solve some multimedia security problems; however, full encryption for multimedia content not only requires a great deal of process time but also is concerned mainly with the access control aspect. And there is another security vulnerability which has not been solved by full encryption technology, when the ciphered social multimedia content is decrypted, the content will be not protected anymore, and the decrypted multimedia is illegal used by some legal user. Digital watermarking is another multimedia security technology, with which the owner may use watermark to monitor illegal copies [3]. Actually, encrypted social multimedia content needs another security technology in order to keep control the use of decrypted content.

* Corresponding Author

ISSN: 1738-9976 IJSIA

There have been some related research works on joint watermarking and encryption recently [4]. D. Bouslimi *et. al.*, proposed a security technology for medical images with joint watermarking and encryption algorithm [5]. In this paper, joint watermarking and encryption are considered together to protect medical images. The authors researched an interactive buyer-seller watermarking protocol for content security [6]. In [7], some wavelet subbands are encrypted and other resolution subbands are used to embed watermark. While in [8], most significant bit planes are encrypted, and watermarks are embedded into other lower significant bit planes. Although, the above joint watermarking and encryption can solve some security problem in content sharing in social network, watermark cannot verify illegal user who redistributed the watermarked copies. Fingerprint information can trace those users who redistribute multimedia content.

Digital fingerprinting can embed a unique mark for one user, and the unique mark is a useful tool to trace redistributed content. Although multimedia fingerprinting and multimedia encryption usually protect multimedia separately, there are some research works [9, 10] combined them for multimedia security. The need to combine multimedia fingerprinting and multimedia encryption keeps rising recently. Kundur *et. al.*, [11] proposed a novel architecture for joint fingerprinting and decryption scheme for multimedia security, with which a better compromise between practicality and security can be achieved. Lian SG *et. al.*, [12, 13] combined fingerprinting, encryption, and encoding to secure multimedia content. In [14], a joint fingerprinting and encryption scheme inspired by the Chameleon cipher was proposed, the proposed joint scheme could provide confidentiality and traceability. In [15], the authors proposed a new genetic fingerprinting scheme for multicast video protection. Joint fingerprinting and decryption (JFD) schemes are proposed for multimedia security [16-18].

All the above schemes can solve part aspect of security problem in multimedia sharing in social network, however, these schemes cannot apply secure social multimedia sharing in social network, because the joint fingerprinting and encryption scheme can produce big data issue, and those JFD schemes will increase the overheads of resource-constrained mobile devices, the complex decryption process in resource-constrained device will decrease the QoE (quality of experience). In this paper, a novel JFE algorithm based on GoL is proposed to balance the shortcoming between JFE and JFD. In fact, GoL can develop chaotic behavior with simple rules, which makes it an interesting technology for image encryption [19]. Simple and fast computation can make it practical for social multimedia sharing in social network.

By using the proposed JFE technique, privacy-preserving and secure content sharing can be achieved. The remainder of this paper is organized as follows. Basic theory is introduced in Section 2, followed by the proposed methods in Section 3, then, the security analysis and experimental results are demonstrated in Section 4, we conclude our paper in Section 5.

2. Basic Theory

2.1. Chaotic Maps

1D Logistic map is described as follows:

$$x_{n+1} = ux_n(1-x_n) \tag{1}$$

where $u \in [0,4]$, $x_n \in (0,1)$, n=0,1,2,… Under the condition that $3.56994 < u \leq 4$, the system will be in a chaotic state.

The PWLCM chaotic map can be described as follows:

$$y_{n+1} = F(y_n, \eta) = \begin{cases} y_n / \eta, & 0 \le y_n < \eta \\ (y_n - \eta)/(0.5 - \eta), & \eta \le y_n < 0.5 \\ 0, & y_n = 0.5 \\ F(1 - y_n, \eta), & 0.5 \le y_n < 1 \end{cases} \quad (2)$$

where $y_n \in (0,1)$, n=0,1,2,…, when control parameter $\eta \in (0,0.5)$, PWLCM system evolves into a chaotic state, y_n and η can be used as a key for encryption and decryption.

2.2. Cellular Automata

Cellular automata are dynamical systems [19], and the (2-D) cellular automata are also called GoL, a GoL consists of a cell matrix, in which each cell has two states: dead and alive. Dead state and alive state are represented by 0 and 1 respectively. Each cell has eight neighbor cells which are horizontally, vertically, or diagonally adjacent. Each cell updates its new state in the next generation with the following transition rules.

(1) Any live cell dies when its live neighbors are fewer than two.

(2) Any live cell which has two or three live neighbors will live continuously.

(3) Any live cell which has more than three live neighbors dies.

(4) Any dead cell will live if it has exactly three live neighbors.

3. The Proposed JFE Scheme

3.1. Encoding with Social Network Analysis

For a multimedia social network, we first identify the hierarchical and overlapping community structure. The community can conduct a social fingerprint code design, and the social tree-structure fingerprint code scheme can reduce the length of code. Assigned to this fingerprint codeward, users who are likely to collude will get codewards which have the same community segment, and the community code segment is regarded as multilevel outer code, the user code for every user is different.

3.2. TSHWT with Social Network Analysis

According to the social fingerprint code, we define the splitting scheme for multi-level TSHWT (Tree Structure Haar Wavelet Transform) with social network analysis. For example, the community structure is presented in Figure 1 ,where the number of community layers is $n+1$, then the outer code' number of level is n, LH and HL subbands for community code embedding will be split into n levels according to Figure 1. As shown in Figure 1, the LL subband is used to embed user code segment. Because all these subbands are independent, then the fingerprint code segments can embed into these subbands parallelly.

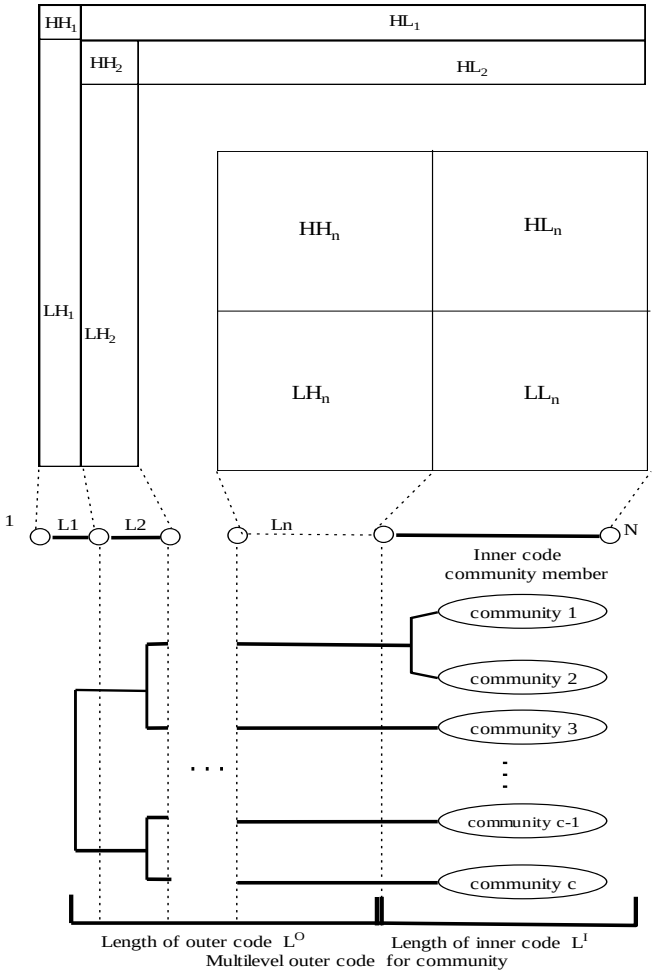


Figure 1. Encoding and TSHWT with Social Network Analysis

3.3. The Parallel JFE Scheme

In parallel computing mode, each PE (processing element) is responsible for joint fingerprinting and encryption to the part of image data. To allow parallel image fingerprinting and encryption, subsets of the image data, namely those wavelet subbands should be independent. In this paper, the subbands are uncorrelated. However, there arise the following additional requirement for parallel JFE scheme:

The total time of a parallel joint fingerprinting and encryption scheme is determined by the slowest PE, since other PEs have to wait until such PE finishes fingerprinting and encryption process. In this paper, the subset of the image data is the subband in TSHWT domain, therefore, slow PE will get small subband. The highest-level approximation subband in TSHWT domain is used to embed the inner code part of fingerprints, and the other coefficients including HL and LH subbands are used to embed the community code segment. First, fingerprint code segment are embedded into subbands with spread-spectrum embedding mechanism concurrently. Then, all fingerprinted contents are encrypted totally via CA permutation process.

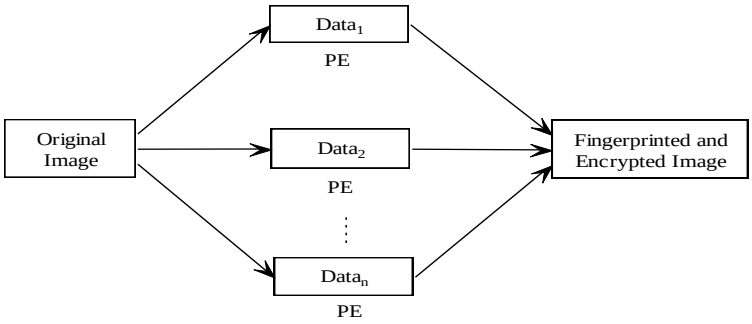


Figure 2. Parallel Computing Mode for Joint Fingerprinting and Encryption

The proposed parallel joint fingerprinting and encryption scheme can be divided into the following steps:

Step 1: According to the social multi-level fingerprint code structure, we decompose the original image I to get the one-level TSHWT coefficient matrix, we can get four one-level sub-bands: the approximation subband LL, and the detailed subband HL, LH, HH, and then the detailed coefficients HL and LH are transformed by TSHWT according to the structure of the community code;

Step 2: Use logistic map to generate a chaotic sequence, with which a two-dimensional grids of cells G^0 can be created, parameters x_0 and u are used as keys. G^0 is used as seed of GoL. With G^0, we can encrypt the TSHWT coefficient matrixes parallelly ;

Step 3: We apply the rules of GoL to produce later generations and put the original coefficients into the encrypted content matrix accordingly;

Step 4: After R rounds iteration, we put the rest of the original coefficients into the encrypted content matrix;

Step 5: To add additional security level, the PWLCM map is used to diffuse the scrambled coefficients. Transform the fingerprinted and permutted coefficient matrix to a one-dimensional vector FP={ fp_0 , fp_1 ,…, fp_{l-1} }. Under the control of $K_{random} = k_0 k_1 ... k_{l-1}$, generate n random sequences m_0 , m_1 , …, m_{n-1} with the PWLCM map. The fingerprinted and permuted content is superposed by the random sequences to yield the encrypted coefficients sequence $cp_0, cp_1, \ldots, cp_{l-1}$, where $cp_i = fp_i + m_i$;

Step 6: Perform ITSHWT reconstruction with the fingerprinted and encrypted coefficients. We can get the protected image.

4. Experiment Results and Security Analysis

4.1. Perceptual Security

The experimental results of the proposed double-level encryption scheme are presented in Figure 4(b). It is very apparent that all the encrypted images are not perceived become of noise-like signal. Therefore, the encrypted scheme is secure.

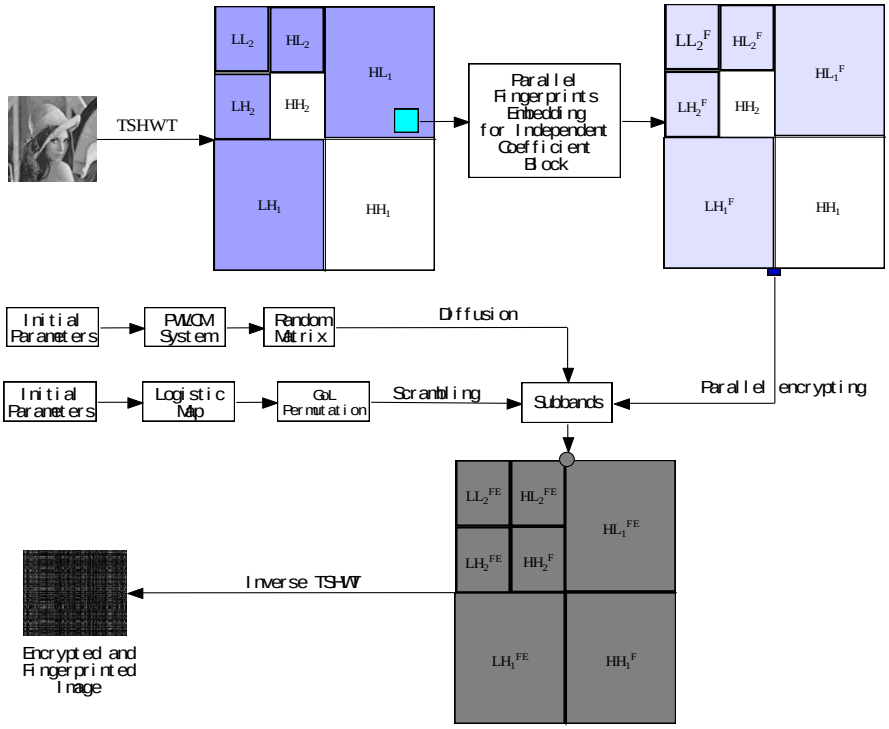


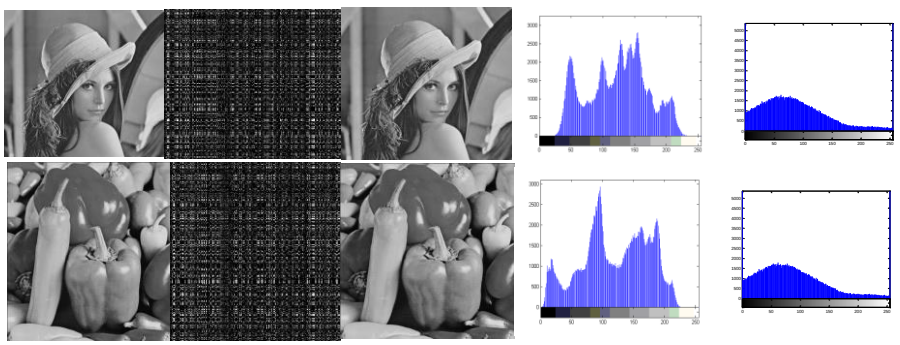
Figure 3. The Architecture of Parallel Image Fingerprinting and Encryption Algorithm

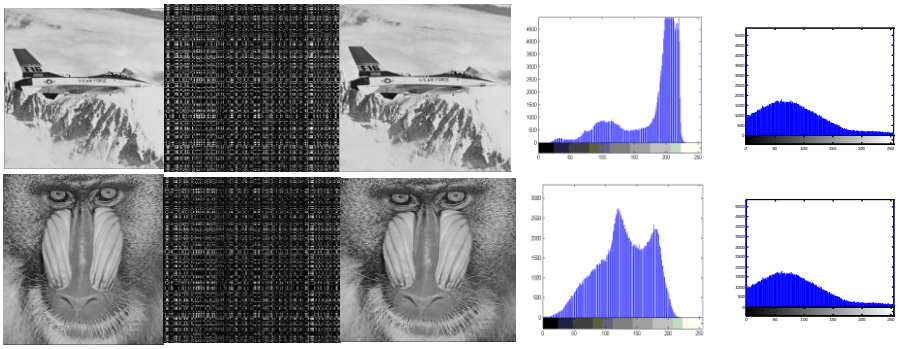
4.2. Imperceptibility of the Fingerprint

The fingerprint information hidden in the image should not be visible. In this paper, the fingerprint code segments are embedded into LL, HL and LH subbands. The fingerprinted images are shown in Figure 4(c), from those images we cannot observe the fingerprint information, and the fingerprinted images are not shown lower visual quality than the original images.

4.3. Resistance to Statistical Attack

To verify the resistance to statistical, the histograms of the original and encrypted images are compared. Figure 5(c), (d) show the grey-scale histograms of the original and encrypted images. According to the two histograms, it's shown that the pixel grey values of the original images are concentrated on some values, but the histograms of the encrypted images are significantly different from the histograms of the original images, and although the histograms of the original images are different, the histograms of the encrypted ones are very similar, which makes statistical attacks difficult. Therefore, the proposed double-level encryption scheme can resist to statistical attack.





(a) (b) (c) (d) (e)

Figure 4. The Experimental Results: (a) The Original Images, (b) The Encrypted Images, (c) The Decrypted Images with Fingerprints, (d) The Grey Histogram of the Original Images, (e) The Grey Histogram of the Encrypted Images

5. Conclusion

In this paper, we propose a novel joint fingerprinting and encryption scheme based on GoL in the TSHWT transform domain to deal with the issues of traitor tracing. The proposed joint fingerprinting and encryption method offers one main contribution: a discussion of how to use GoL for secure social multimedia sharing with social network analysis. The experimental results and security analyses demonstrate that the proposed scheme possesses perceptual security and can resist statistical attacks.

Acknowledgements

This work is supported by the NSF of China under Grant No. 61502154,61370092 and 61370223, Natural Science Foundation of Hubei Province of China (No. 2015CFB236, 2014CFB188), and Youth innovation team project in Hubei Provincial Department of Education (No. T201410).

References

[1] T. Thomas, S. Emmanuel, A. Subramanyam and M. S. Kankanhalli, "Joint watermarking scheme for multiparty multilevel DRM architecture", *Information Forensics and Security, IEEE Transactions on*, vol. 4, **(2009)**, pp. 758-767.
[2] H. Cheng and X. B. Li, "Partial encryption of compressed images and videos", *Ieee Transactions on Signal Processing*, vol. 48, **(2000)** Aug, pp. 2439-2451.
[3] E. Ganic and A. M. Eskicioglu, "Robust DWT-SVD domain image watermarking: embedding data in all frequencies", in *International Multimedia Conference: Proceedings of the 2004 workshop on Multimedia and security*, **(2004)**, pp. 166-174.
[4] R. Gupta and S. Jain, "A review on watermarking techniques for compressed encrypted images," in *Medical Imaging, m-Health and Emerging Communication Systems (MedCom), 2014 International Conference on*, **(2014)**, pp. 10-13.
[5] D. Bouslimi, G. Coatrieux and C. Roux, "A joint encryption/watermarking algorithm for verifying the reliability of medical images: Application to echographic images", *Computer Methods and Programs in Biomedicine*, vol. 106, **(2012)**, pp. 47-54.
[6] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol", *Image Processing, IEEE Transactions on*, vol. 10, **(2001)**, pp. 643-649.
[7] S. Lian, Z. Liu, R. Zhen and H. Wang, "Commutative watermarking and encryption for media data", *Optical Engineering*, vol. 45, **(2006)**, p. 080510.
[8] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. De Natale and A. Neri, "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain", *Signal Processing: Image Communication*, vol. 26, **(2011)**, pp. 1-12.
[9] J. Guo, P. Zheng and J. Huang, "Secure watermarking scheme against watermark attacks in the encrypted domain", *Journal of Visual Communication and Image Representation*, vol. 30, **(2015)**, pp. 125-135.

[10] A. Qureshi, D. Megías and H. Rifà-Pous, "Framework for preserving security and privacy in peer-to-peer content distribution systems", *Expert Systems with Applications*, vol. 42, **(2015)**, pp. 1391-1408.
[11] D. Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rights management", *Proceedings of the IEEE*, vol. 92, **(2004)**, pp. 918-932.
[12] S. Lian and Z. Wang, "Collusion-traceable secure multimedia distribution based on controllable modulation", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 18, **(2008)**, pp. 1462-1467.
[13] S. Lian and X. Chen, "Traceable content protection based on chaos and neural networks", *Applied Soft Computing*, vol. 11, **(2011)**, pp. 4293-4301.
[14] A. Adelsbach, U. Huber and A. R. Sadeghi, "Fingercasting–Joint Fingerprinting and Decryption of Broadcast Messages", *Transactions on data hiding and multimedia security II*, **(2007)**, pp. 1-34.
[15] H. C. Huang and Y. H. Chen, "Genetic fingerprinting for copyright protection of multicast media", *Soft Computing-A Fusion of Foundations, Methodologies and Applications*, vol. 13, **(2009)**, pp. 383-391.
[16] C. Y. Lin, P. Prangjarote, L. W. Kang, W. L. Huang and T. H. Chen, "Joint fingerprinting and decryption with noise-resistant for vector quantization images", *Signal Processing*, **(2012)**.
[17] B. Czaplewski and R. Rykaczewski, "Matrix-based robust joint fingerprinting and decryption method for multicast distribution of multimedia," *Signal Processing*, vol. 111, **(2015)**, pp. 150-164.
[18] M. Li, D. Xiao, Y. Zhang and H. Liu, "Attack and improvement of the joint fingerprinting and decryption method for vector quantization images", *Signal Processing*, vol. 99, **(2014)**, pp. 17-28.
[19] S. Wolfram and M. Gad-el-Hak, "A new kind of science", *Applied Mechanics Reviews*, vol. 56, **(2003)**, p. B18.

Authors

Conghuan Ye, received the B.S. and M.S. degree in computer science from Hubei Normal University, Hubei, China, in 2002, and University of Electronic Science and Technology of China, Chengdu, Sichuan, China, in 2005, respectively. Now, his research interests include digital fingerprinting, digital right management, complex network, and cloud computing. Dr. Ye received the scholarship from UESTC from 2003 to 2004.

Dr. Ye has co-authored over 30 publications including book chapters, journal and conference papers. He received the Ph.D. degree in computer science and technology, Huazhong University of Science and Technology (HUST) in 2013, Wuhan, Hubei, China. Since 2013, he has been an associate professor with the college of computer science and technology, HBEU.

Zenggang Xiong, received the MA degree from Hubei University, China, in 2005, and the PhD degree in computer science from Beijing University of Science and Technology, China, in 2009. He is now a professor in Hubei Engineering University. His research interests are in the areas of peer-to-peer computing, Cloud computing, distributed systems and big data.

Yaoming Ding, received the MA degree from Huazhong Normal University, China, in 2000, and the PhD degree in education from Huazhong Normal University, China, in 2011. He is now a professor in Hubei Engineering University. His research interests are in the areas of optical communication technology and cloud computing.

Xuemin Zhang, received the Bachelor degree in computer science from Hubei Normal University, China, in 2001, and the MA degree in computer science from Wuhan University of Technology, China, in 2009. She is now an associate professor in Hubei Engineering University. Her research interests are in the areas of Cloud computing, distributed systems, Service Computing. She is a member of the IEEE and the ACM.

Guangwei Wang, received the B.S. and M.S. degree in computer science from Huazhong Normal University, Wuhan, China, in 2005 and 2008, respectively. He received the Ph.D. degree from Huazhong University of Science and Technology in 2012. Now, He works in School of Computer and Information Science, Hubei Engineering University and his research interests include Computer vision and video analysis. He has co-authored more than 10 papers published in various journals.

Fang Xu, received the B.S. and M.S. degree in computer science from Hubei Engineering University, Hubei, China, in 2003, and Wuhan University, Wuhan, Hubei, China, in 2009, respectively. Now, his research interests include Mobile Social Networks, digital fingerprinting, Machine Learning, and cloud computing.

Dr. Xu has co-authored over 20 publications including journal and conference papers. He is currently a Ph.D. student in the Wuhan University at Wuhan, majoring in computer science and technology.

Kaibing Zhang, received the M.Sc. degree in Computer Software and Theory from Xihua University, Chengdu, China, in 2005 and the Ph.D. degree from Xidian University, Xi'an, China, in 2012, respectively. He is currently an Associate Professor at the School of Computer and Information Science, Hubei Engineering University, Xiaogan, China. From 2013, he is a Post-Doctoral Research Fellow with the School of Electronic Engineering, Xidian University, Xi'an, China. His main research interests include pattern recognition and computer vision.