International Journal of Security and Its Applications
Vol. 10, No. 4 (2016), pp.279-288
http://dx.doi.org/10.14257/ijsia.2016.10.4.26

Secure Multimedia Content Distribution for M2M Communication

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

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

Abstract

Multimedia content distribution based on M2M communication is attracting increasing attentions nowadays. Considering that multimedia will be widely used in various applications over M2M network, the wide range of multimedia content and M2M devices has raised new security requirements for multimedia communication. In this paper, we focus on an aspect of DRM that involves secure multimedia distribution which combines multimedia encryption, copy detection, and digital fingerprinting to prevent widespread piracy. Multimedia encryption is used to encrypt multimedia content firstly before distribution, then, Copy detection is used to verify whether a protected multimedia content is a redistributed copy of its or no, At last, digital fingerprinting is introduced to protect multimedia content further. In this paper, we first use using encryption, fingerprinting and copy detection for secure distribution in M2M communication environments. The secure effect of the proposed scheme has been verified through theory analysis and experimental results.

Keywords: *M2M communication; Multimedia fingerprinting; Multimedia security; Multimedia distribution; Multimedia encryption*

1. Introduction

With the fast advance of communication technology and the dramatic penetration of embedded devices, including smart phones, Ipads, TVs, laptops, speakers, and electronic appliances, the machine-to-machine (M2M) network technology has become an important field to connect with groups of devices and systems. M2M network is a very important platform for multimedia communication. Aim at enabling interactions between devices ranging from wireless sensors to robots, M2M communication often reduces the cost of information acquisition manually, or offers multimedia services based on M2M device.

Multimedia content distribution is an important service in M2M communication environments. The users hope to distribute multimedia content to M2M devices, and they wish to enjoy the content distribution easily and conveniently. M2M communication is used for automatic content transmission from remote sources such as Ipad, smart phone, *etc*. It makes multimedia content exchangeable among machinery equipment, people, and the controlling system automatically. M2M communication network plays an important role in exchange multimedia content such as audio, video, photos among individuals. Such an open communication network lead serious multimedia security problems during M2M communication. How do consumers determine that M2M system is secure for multimedia content exchange? In fact, the research in multimedia communication security for M2M network is in the initial stage [1].

* Corresponding Author

ISSN: 1738-9976 IJSIA

To establish a secure multimedia communication environment for M2M network, a number of multimedia security technologies are desirable. Concerned about the consequences of piracy of multimedia data, owners are interested in encryption, digital watermarking, and multimedia authentication which can protect their content from illegal use [2]. Encryption can prevent an unauthorized access. The paper [3] provided a survey of multimedia content scrambling algorithms based on partial encryption. Multimedia encryption cannot trace any illegal redistribution, so Conghuan Ye [4] proposed a traceable content distribution scheme to trace traitor efficiently.

There are some existing works addressing multimedia communication security. In [5], some means such as lightweight packet encryption, fingerprinting, and desynchronization are proposed to provide a security multimedia distribution scheme for IPTV. In [6], the multimedia content is modulated to generate the unintelligible content at the server side, and then the fingerprinted multimedia content is produced under the control of the fingerprint code at the client side. In [7], a digital fingerprinting scheme distributes the same encrypted content to different user and decrypts the encrypted content into a different fingerprinted copy with different decryption keys. Kang [8] researched a secure stream media distribution scheme to improve the bandwidth efficiency. D. Megias presented a P2P multimedia content distribution framework [9, 10]. In the letter [11], Hu and Li propose an efficient asymmetric multimedia fingerprinting scheme. The authors [12] have proposed a method to decide those who are the redistributor.

Nowadays, on one hand, multimedia content is used more and more throughout our daily life because of advance of M2M communication. On the other hand, M2M networks users wish to access multimedia content conveniently. Media devices that contain resources should preprocess their multimedia resources to protect privacy. In other words, the media device should manage, control, process and render multimedia content before the content is transmitted from the device and presented to the M2M network. Therefore, if authorized consumers consume contents in M2M systems, the contents need to be adapted for meet the demand of users, multimedia content distribution systems have to provide functionalities for users' authentication [13]. However, there is no related works which resolved the secure content distribution in M2M communication environment.

Therefore, efficient multimedia protection strategy is needed to avoid multimedia security problem in M2M network environment. In this paper, the authors propose a security framework which combines encryption, fingerprinting/watermarking and copy detection. The paper is organized as follows. Section 1 introduces the background, and Section 2 presents framework of secure multimedia content distribution in M2M networks. Experimental results is mainly shown in Section 3, at last, the conclusion of the paper is presented in Section 4.

2. Distribution Scheme

Base on the security demand of M2M communication, an elementary framework of secure content distribution is shown in Figure (1). The initializing media device that owns content transmits a request message to content index server, claiming for register of content and then request to distribute multimedia to users. The basic character of multimedia content and the receivers are included in the request message. The content index server will communicate with the multimedia processing server for content protection and asking for distribution of the content. The content distribution is based on multicast transmissions.

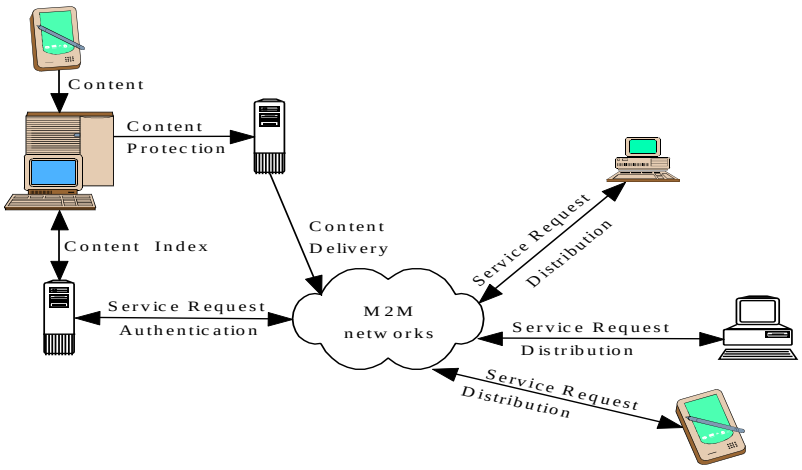


Figure 1. Framework of Secure Content Distribution

2.1. Multimedia Content Authentication Scheme

Multimedia communication security over the existing open wired and wireless M2M networks has become an important research field. The inappropriate security techniques can burden the multimedia content index server and the multimedia processing server with excessive preprocessing which may reduce the visual quality and does not meet security requirement.

Because steganography, multimedia encryption and copy detection realize different security functionalities, they can be combined together to protect both the confidentiality and the identification. Encryption obscures the multimedia content. Fingerprinting realize the traitor tracing. Copy detection develops automated content authentication.

2.1.1Traditional scheme: The traditional content authentication scheme is shown in Figure (2). First, multimedia content owner embeds the watermark information into the multimedia content. After that, the watermarked multimedia data is encrypted in the sender side. Then, the encrypted content with copyright information of the owner is distributed to users through M2M networks. At last, the encrypted multimedia content is distributed to users.

In the framework, when an illegally distributed copy is found, copy detection will authenticate the copyright with the following steps: First, the content owner extracts the feature of watermarked multimedia content. The feature, which is much smaller in size compared with the original multimedia content. Then, the feature is stored in the content index database. In the end, once the similar multimedia content is found in M2M networks later, a piece of mark information is extracted from the tracked multimedia content, and compare mark information with the copyright information of the owner. If the mark is the copyright information of the owner, the content is copyright protected. Otherwise, the feature of the tracked content is extracted, the feature is used to authenticate the suspicious content is the copy of original multimedia content or not. The suspicious content may be the attacked version of the original.

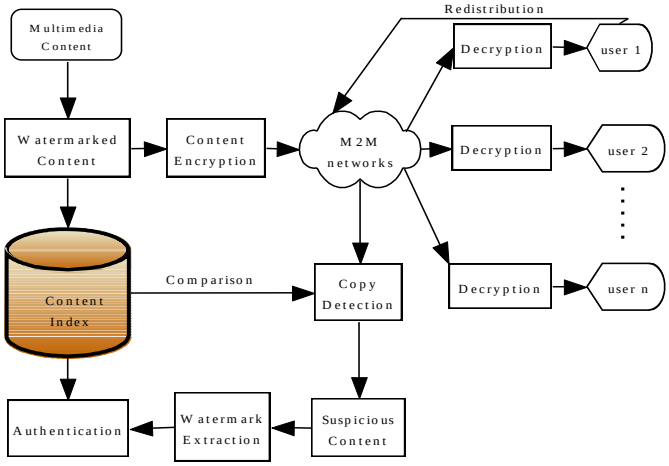


Figure 2. Multimedia Content Distribution and Copyright Authentication Scheme

(2) New traceable content authentication scheme: Digital watermarking cannot authenticate the one who redistributed the content. Digital fingerprinting can track the redistribution of digital multimedia. Fingerprint information can deter redistribution by embedding a unique serial number into each distributed copy before multimedia content is distributed to users through M2M communication.

Once a similar multimedia content is detected somewhere, the fingerprint information is extracted, with the fingerprint information, the related detector will decide an illegal user or not. Therefore, at sender side, the multimedia content is embedded fingerprints instead of watermarks during the watermarking process as Figure (3) shows.

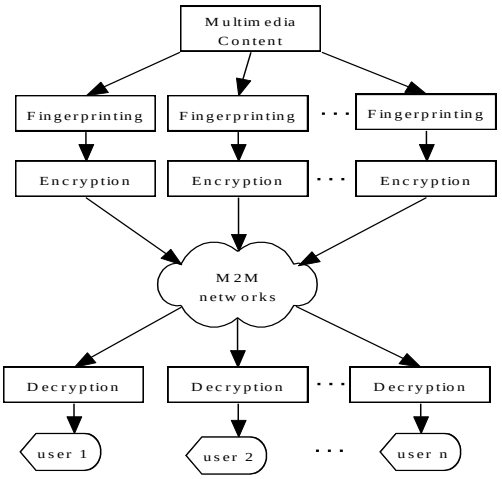


Figure 3. Trackable Multimedia Content Protection and Distribution Scheme

2.2 The Steganography Scheme

Steganography techniques have been developed for images, audio, and video [14]. This section will introduce two steganography techniques: watermarking and fingerprinting.

2.2.1 The Watermarking Scheme: Digital watermarking technology plays an important role in multimedia content protection and related fields. Ownership of multimedia content can be established by extracting the inserted watermark. Therefore, digital watermarking is an attractive solution for copyright protection.

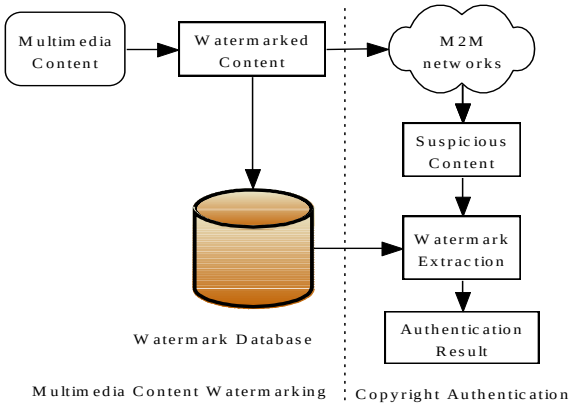


Figure 4. Watermarking Scheme for Multimedia Content Protection

In watermarking-based steganography technique [21], a piece of same mark information is imbedded into multimedia content, then the watermarked multimedia content is distributed to users with multicast technology [15]. The watermark information can be copyright information, which can authenticate the owner of the multimedia content. However, there are also apparent disadvantages: watermark can not authenticate somebody who redistributed the copies.

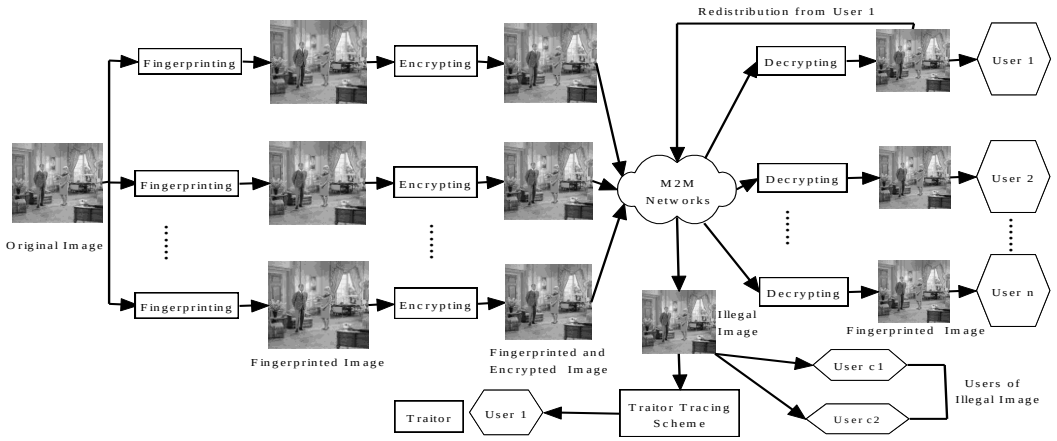


Figure 5. Fingerprinting Scheme for Multimedia Content Protection

2.2.2 The Fingerprinting Scheme: Digital fingerprinting is another major application of digital watermarking. A piece of digital fingerprint information can represent a unique user, so different users own different fingerprint information, so the fingerprint information can identify those who redistribute the original multimedia. When the multimedia content is prepared to distribute into M2M network, fingerprint information is embedded into the multimedia content, then the fingerprinted multimedia content is distributed to user. Illegal traitor detection will deter users from redistributing multimedia content. The fingerprinting process and traitor tracing are shown in Figure (5).

2.3 Multimedia Encryption

Security requirements of multimedia content must be met when multimedia content is distributed from an initial M2M device to target M2M devices [16-18]. As one of the major scheme of secure multimedia content distribution over M2M network, multimedia encryption can protect content from illegal access. In fact, multimedia encryption scheme as shows in Figure (6) should compose of two iteration processes: confusion process (shuffling the positions) and diffusion process (changing the values). The confusion stage

permutes the positions of the selective pixels, without changing their values. The values of selective part of multimedia are modified sequentially in the diffusion stage; at last a little change in a plaintext poses as much part change in the encrypted content as possible.

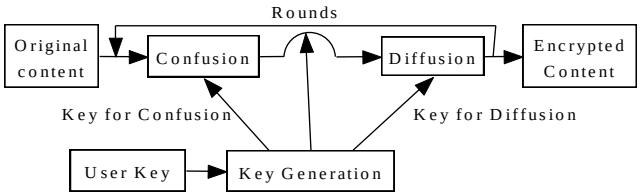


Figure 6. Multimedia Content Encryption Architecture

As a frequently used architecture to encrypting multimedia, the confusion and diffusion can also be processed in the frequency domain. In order to obtain high level multimedia communication security, multimedia encryption methods can be used to scramble the selective part of multimedia in spatial and transform domains, respectively. In this case, the frequency transform can increase burden of server [19]. Chaotic system is a good way favorable to secure multimedia communications because of their significant features such as parameter sensitivity and ergodicity.

2.4 Multimedia Content Copy Detection Scheme

Encryption can provide multimedia communication security; however, it will be lose efficacy when the encrypted content is decrypted, then, the decrypted content will be redistributed conveniently. But copy detection technique can provide copyright protection persistently.

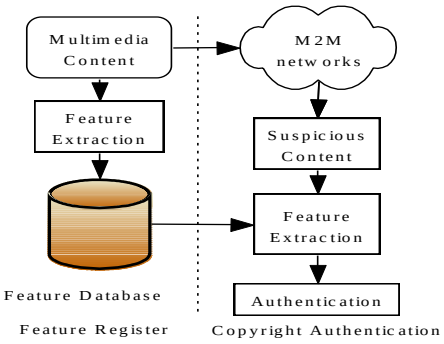


Figure 7. Copy Detection for Copyright Authentication

The feature detector compares the feature of the similar image with the original feature to authenticate copy [20]. The copy detection framework is shown in Figure (7). The detection method is based on CBCD (Content Based Copy Detection) [21]. An original feature which is registered in feature database through extracting a feature vector representing the original multimedia content. To decide whether a multimedia is registered or not, the feature of the multimedia content is extracted and compared with the ones stored in the feature database. The comparison results show the multimedia content is a copy or not. The feature database, as shown in Figure (5), stores the feature vectors of the registered multimedia and some labels. The extracted feature should have certain properties: distinguishability and robustness.

3. Results

The experimental result of the proposed combined scheme is demonstrated in this section. Selective encryption based on diffusion and permutation is used to encrypt images. For multimedia security, perceptual security is a major factor to evaluate. In this paper, only a small amount of data are used for encryption, and the encryption results are shown in Figure (8). The multimedia selective encryption will bring some benefits for M2M devices because they are resource-constraint because of manufacturing cost.

3.1. Perceptual Security

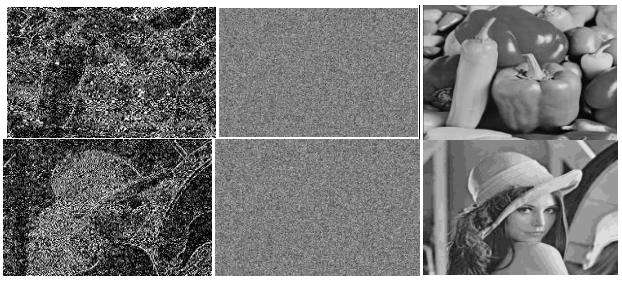
In fact, the encrypted content should not be perceived. In this paper, the original images are encrypted by permutation firstly, and then another chaotic sequence is superimposed to the permuted sequence. The encrypted images are shown in Figure (8). It can be seen that the images encrypted are actually unintelligible in comparison with the original image. Therefore, the proposed scheme indeed possessed high perceptual security.

3.2. Fingerprint Imperceptibility

The fingerprint information, which is embedded into the encrypted content, should not be perceptible. The visual quality of the decrypted content should not be affected by fingerprint information that is hidden in the content. The decrypted fingerprinted images are shown in Figure (8). From Figure 8(c), we can perceive that the decrypted fingerprinted images do not have apparent decrease of visual quality.

3.3. Encryption Process

The encrypted process includes two stages: permutation and diffusion. And they are independent with each other. Therefore, even if the permutation is cracked, the traitor still cannot decrypt the image because of the diffusion process. Figure (8) shows the comparison of the two kind of encrypted images. It is very clear that the permutation process in the proposed scheme can enhance perceptual security. Therefore, the proposed scheme is effective for secure content sharing.



(a) (b) (c)
(a) Only LL-level Coefficients Permutation,
(b) Permutated Whole Images with LL-level Coefficients Diffusion,
(c) Decrypted Fingerprinted Images.

Figure 8. Content Encryption

3.4. Encryption Efficiency

In the case of M2M multimedia communication, it is not considered a feasible technique for multimedia encryption if the encryption and decryption process takes a long time. The time efficiency is depicted in Table 1. From the table, it is clear that time taken

for the encryption process is completed in 0.5 s or so. Therefore, we can say that the proposed scheme for M2M multimedia communication is time efficient.

Table 1. Time Efficiency

Images	lena	peppers	airplane	baboon	watch
Time(s)	0.56	0.52	0.47	0.54	0.52

4. Conclusion

The proliferation of multimedia content exchange on the M2M network presents a challenge in the field of copyright protection, as the unauthorized duplication and distribution of multimedia content become easier. In this paper, a secure multimedia content distribution mechanism is proposed, the scheme combines encryption, fingerprinting, and copy detection to address content protection, authentication respectively. To deter legitimate users from illegally redistributing the decrypted content, the scheme employs the ideas of joint copy detection and fingerprinting to deter content redistribution. Copy detection uses the content itself rather than other information to verify whether a protected multimedia content is a redistributed copy of its or no. Fingerprinting of multimedia content using digital watermarks is an effective means of determining original owners of pirated copies. In the end, the novel scheme can trace down the distributor via the fingerprinting signal.

Acknowledgments

This work is supported by NSF of Hubei Province of China (No.2015CFB236), and Youth innovation team project in Hubei Provincial Department of Education (No.T201410) , and NSF of China Grants (61502154, 61370092, 61370223).

References

[1] Rongxing Lu, Xu Li, Xiaohui Liang, and Xuemin. GRS: The Green, Reliability, and Security of Emerging Machine to Machine Communications. IEEE Communications Magazine 2011; 49: 28-35.
[2] E. T. Lin, *et al*.. Advances in digital video content protection. Proceedings of the IEEE 2005; 93: 171-183.
[3] D. Kundur and K. Karthik. Video fingerprinting and encryption principles for digital rights management. Proceedings of the IEEE 2004; 92: 918-932.
[4] C. Ye, J. Li, and Z. Xiong. Traceable Content Distribution Using Wavelet Decomposition and Social Network Analysis. 2012 International Symposium on in Computer, Consumer and Control (IS3C) 2012: 789-792.
[5] S. G. Lian and Z. X. Liu. Secure media content distribution based on the improved set-top box in IPTV. IEEE Transactions on Consumer Electronics 2008; 54: 560-566.
[6] S. G. Lian and Z. Q. Wang. Collusion-Traceable Secure Multimedia Distribution Based on Controllable Modulation. IEEE Transactions on Circuits and Systems for Video Technology 2008; 18: 1462-1467.
[7] S. G. Lian. Secure image distribution based on joint decryption and fingerprinting. Imaging Science Journal 2009; 57: 84-93.
[8] KANG Shou-qiang, ZHENG Jian-yu, WANG Yu-jing, JI Bin, LAN Chao-feng, GAO Hua-qiang. A Streaming Media Secure Communication Method Combined by Dynamic Key of Dual Chaotic Systems and RSA. Journal of Harbin University of Science and Technology, 2015,20(4), 109-115.
[9] D. Megias. Improved Privacy-Preserving P2P Multimedia Distribution Based on Recombined Fingerprints. IEEE Transactions on Dependable and Secure Computing 2015; 12: 179-189.
[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 2015; 42: 1391-1408.
[11] D. F. Hu and Q. L. Li., Asymmetric Fingerprinting Based on 1-out-of-n Oblivious Transfer. IEEE Communications Letters 2010; 14: 453-455.
[12] H. Nakayama, *et al*., Network-Based Traitor-Tracing Technique Using Traffic Pattern. IEEE Transactions on Information Forensics and Security, 2010; 5: 300-313.

[13] A. Carreras, E. Rodriguez, J. Delgado, S. Dogan, H. K. Arachchi, A. M. Kondoz, *et al*., Architectures and technologies for adapting secured content in governed multimedia applications. IEEE MultiMedia 2011;18: 48-61.
[14] Petitcolas FAP, Anderson RJ, Kuhn MG. Information hiding - A survey. Proceedings Of The IEEE 1999;.87: 1062-1078.
[15] T. Bianchi, A. Piva. Secure watermarking for multimedia content protection: A review of its benefits and open issues. IEEE Signal Processing Magazine 2013; 30: 87-96.
[16] Chen GR, Mao YB, Chui CK. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons & Fractals 2004;21: 749-761.
[17] M. Ghebleh, A. Kanso, and H. Noura. An image encryption scheme based on irregularly decimated chaotic maps. Signal Processing: Image Communication 2014; 29: 618-627.
[18] J. A. E. Fouda, J. Y. Effa, S. L. Sabat, and M. Ali. A fast chaotic block cipher for image encryption. Communications in Nonlinear Science and Numerical Simulation 2014;19:578-588.
[19] A. Pande, P. Mohapatra, and J. Zambreno. Securing multimedia content using joint compression and encryption. IEEE MultiMedia, , 2013; 20:50-61.
[20] W.-L. Zhao and C.-W. Ngo. Flip-invariant SIFT for copy and object detection. IEEE Transactions on Image Processing 2013; 22: 980-991.
[21] G. Awad, P. Over, and W. Kraaij. Content-based video copy detection benchmarking at TRECVID. ACM Transactions on Information Systems (TOIS) 2014; 32:1-14.

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 50 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.