An Efficient and Impartial Buyer-Seller Watermarking Protocol

Xinchun Cui[1], Gang Sheng[2], Fengyin Li[1], and Xiaowu Liu[1]
[1] School of Information Science and Engineering, Qufu Normal University, Rizhao Shandong, 276826, China
[2] School of Management, Qufu Normal University, Rizhao Shandong, 276826, China
Email: cuixc@nuaa.edu.cn; rzshenggang@163.com; {lfyin318, ycmlxw}@126.com

Abstract — Buyer-seller watermarking protocols are designed to deter clients from illegally distributing copies of digital content. To be efficient and fair is important to buyer-seller protocols. In this paper, an anonymous and interactive buyer-seller protocol is proposed, which is designed to be impartial and efficient. To solve the unbinding problem and the buyers' right problem, operations of watermark insertion and digital content selling are performed by a Trusted Third Party in the proposed scheme. Buyers and sellers have equal rights and responsibilities, and computational and corresponding overhead is reduced. We show that the proposed protocol is fair, secure and efficient.

Index Terms—Copyright protection, buyer-seller protocol, unbinding problem, the buyers' right problem

I. Introduction

With rapid growth of the Internet technology, digital data (images, audios, videos and database files) can be acquired easily. On the one hand, this helps people to share digital products with others. On the other hand, illegally copies are produced and distributed with little efforts. To deter pirate and protect the copyright of digital products, digital watermarking technology [1]-[6] is introduced. A digital watermark is an imperceptible signal added to digital data before selling, which can be detected later for buyer/seller identification, ownership proof, traitor tracing and so forth.

However, watermarking technology can be effective only if it is applied by employing specific "watermarking protocols," which define the scheme of the interactions that have to take place among the entities involved in the purchase processes. Most watermarking protocols are based on public-key cryptography systems. Among them, symmetric watermarking protocols are the first proposed ones. The main defect of them is the "buyers' right problem," which was first indicated by Qiao in Ref. [2]. To overcome this shortcoming, asymmetric watermarking protocols were designed [7], [8]. Later on, anonymous fingerprinting scheme was introduced to keep the privacy of customers [9], [10]. Recently, buyer-seller protocols that utilize the concepts of secure watermark embedding were proposed [11], [12].

Unfortunately, most of the above protocols are directed by a seller [7], [10], [13], [14] or seller favored, that is, either a seller embeds the watermark into a digital data or holds a watermarked copy. So, by making analysis and modification on the data she (or he) holds, a malicious seller can accuse a innocent buyer of piracy. That is unfair to an honest buyer. Yet it is of the utmost importance for a protocol to be fair to all of its partners.

The purpose of this research is to propose an impartial buyer-seller watermarking protocol that favors neither the seller nor the buyer. So we will concentrate on the fairness and efficiency of the proposed protocol, none of detailed techniques will be specified. The proposed protocol can be implemented with any watermark embedding scheme, and it is suitable to any kind of digital resources, such as images, audio, videos and database files. The rest of this paper is structured as follows. We review the related researches in Section II. In Section III, we describe the proposed buyer–seller watermarking protocol in details. Security issues of the proposed protocol are examined in Section IV. Finally, the conclusion is given in Section V.

II. Related Researches

There are rich studies in the literature of digital copyright and traitor tracing. We will review some related ones.

Wagner proposed a symmetric fingerprinting scheme in 1983 [1]. In this scheme, a seller embeds the buyer's identity in his contents by himself for traitor tracing. As the seller possesses each copy that she has sold, a malicious seller can accuse an innocent buyer of illegal distribution. This is distinguished as the "buyers' right problem" in Ref. [2]. To overcome this problem, Qiao and Nahrstedt [2] has proposed an *owner–customer watermarking protocol*. In this scheme, the buyer first encrypts a predetermined sequence of bits with a secret key only known to him, and sends the encrypted sequence to the seller (owner). On receiving this sequence, the seller embeds it into his digital content and sends the watermarked copy back to the buyer. Since only the buyer knows the secret key, he can prove to anyone his legitimate possession of the watermarked copy. Unfortunately, as the seller still has access to the

Manuscript received February 16, 2015; revised May 10, 2015.
This work was supported by the Foundation of Research Project of Humanities and Social Science of Ministry of Education of China under grant No.11YJCZH021.
Corresponding author email: cuixc@nuaa.edu.cn
doi:10.12720/jcm.10.5.339-344

watermarked copy in its final form, it is unreasonable to accuse the buyer pointed by the embedded watermark. That is to say, the "buyers' right problem" is not well avoided. Consequently, a seller can not prove his innocent when a pirated copy is found.

Memon and Wang presented an interactive buyer–seller protocol using dual watermarking [7]. In this protocol, a trusted watermark certification authority (WCA) is introduced to generate random watermarks. When the buyer applies, the WCA generates a random but valid watermark, encrypt it using the buyer's public key and the sends it to the buyer. On receiving this, the buyer sends it to the seller. The seller first generates a unique watermark for this transaction, and inserts it into the content as the proof of ownership. This is the first watermark. Then the seller generates a random permutation and uses it to permute the elements of the encrypted watermark received from the buyer. He then inserts the permuted watermark obtained above as a second watermark into the already watermarked digital content, and sends it to the buyer. In this scheme, the seller does not get to know the exact watermarked copy that the buyer receives; hence, he has no chance to create illegal copies that containing the buyer's watermark. So that the buyer cannot claim that an unauthorized copy may have originated from the seller. However, in case the seller finds an unauthorized copy, she can identify the buyer from whom this unauthorized copy has originated and furthermore also prove this fact to a third party by detecting the second watermark. This protocol successfully solves the *customer's right problem* since the watermark insertion operation is performed in the encrypted domain and thus the seller has no access to the watermarked copy of the digital content in its final form. Yet the protocol requires the suspected buyer to decrypt the encrypted watermark in dispute resolution phase, while the buyer may be unlikely to cooperate, this makes the protocol impracticable. Furthermore, the protocol suffers from the "unbinding problem" [10].

In 2004, Lei *et al*. proposed a buyer-seller watermarking protocol derived from Memon and Wong's protocol [10], which solves both the customer's right problem and the *unbinding problem*. In the proposed watermarking protocol, the operations of watermark insertion are performed by the seller rather than by the watermark certification authority.

In 2007, Frattolillo proposed a web-oriented and interactive anonymous buyer–seller watermarking protocol based on homomorphic public-key encryption [13]. In this protocol, when the content provider (seller) receives a series of fingerprinting codes, he encrypts them and the digital content to be sold. Then he sends them to the protection center (PC, serves as the trusted third party). PC chooses one of the encrypted fingerprinting codes and forward it to a service provider (SP), who will embed the fingerprint and feedback a watermarked content. This copy is send to the buyer with the permission of the seller, and relative certificates assigned to the buyer and the seller respectively. This scheme successively solved the "unbinding problem". Yet the seller still has access to the fingerprint, so that malicious sellers may produce fingerprinted copies, distribute them, and claim being pirated. This is referred as another kind of "users' right problem".

In 2008, Katzenbeisser *et al.* proposed a buyer-seller protocol that utilizes the concepts of secure watermark embedding [14]. In this protocol, the seller gets an encrypted watermark, embeds it into the content using a secure watermark embedding approach based on partial encryption [11], [12]. Then, he sends it to the buyer. The buyer uses secure embedding approach to obtain a watermarked version of the content. In contrast to the known solutions, which use homomorphic public-key encryption on the content and impose unpractical constraints on computational resources and transmission bandwidth, this protocol is efficient due to the use of secure embedding algorithms.

To sum up, in all of the above protocols, with or without a WCA, we can see that in most of the proposed watermarking protocols the seller directs the watermarking procedure, and he either has full access to the watermarked content[2] or has partial of it [7],[10], [13], [14].

Thus there exists the possibility that a malicious seller can frame an honest buyer. Furthermore, the "customer's right problem" and the "unbinding problem" are not well resolved. So they are not fair protocols to both the seller and the buyer. This is the very reason that we start this research.

III. Proposed Scheme

The proposed watermarking protocol consists of four sub-protocols. In this section we first describe the model and goals of proposed watermarking protocol, we then illustrate the sub-protocols one by one.

A. Model and Design Goals of Proposed Watermarking Protocol

The model of proposed watermarking protocol is a three party scheme, which includes a seller, a buyer and an authentication center.

(1) The seller (*S*), who wants to make a profit on the sales of certain digital content he owns. She may be the rightful owner of the original digital content, or an authorized reselling agent.

(2) The buyer (*B*) who wants to purchase a copy of the digital content from *S*. He may be a person or an agency.

(3) Authentication Center (*AC*), who is a trusted third party. He supervises the whole procedure of the purchase, applies to all applications, generates and embeds watermarks, and assigns digital certifications.

The goals of the proposed watermarking protocol are as follows [10], [13], [14].

1) The proposed watermarking protocol should be fair to both *S* and *B*. That is, the proposed protocol should guarantee that neither *S* have any chance to frame *B*, nor

B can successfully remove the watermark embedded in any copy he purchased.

2) The proposed watermarking protocol should solve both the "customer's right problem" and the "unbinding problem".

3) The proposed watermarking protocol should allow buyers to keep their identities anonymous during the execution of the protocol;

4) The proposed watermarking protocol should guarantee that both *S* and *B* are undeniable to his(her) activities under this protocol.

5) The proposed watermarking protocol should resist to a secondhand watermark attacks, in which a malicious buyer insert a secondhand watermark to the content he buys and claim the ownership of it.

6) The proposed watermarking protocol should be independent to watermark schemes.

To achieve these goals as well as making the developed watermarking protocol flexible so as to be suited for traitor tracing, we have the following assumptions:

1) The Authentication Center is fully trusted authority (it's a trusted third party);

2) All information is transmitted via secure channel;

Notations used in this paper are listed in Table I.

TABLE I: NOTATIONS USED FOR THE WATERMARKING PROTOCOL

Notation	Meaning
(pk_j,sk_j)	A public-private key pair, pk_j, sk_j denote the public key and private key respectively
$Sign_J(M)$	Signature of message *M* signed by J with his private key
$Cert_J$	The digital certificate issued to subject by authority center
$Tran_{ID}$	Transaction identifier of number *ID*
$E_{pkI}(J)$	The ciphertext of message *J* encrypted with *I*'s public key
IDC	Identifier of a digital content
TS_J	Time Stamp of *J*
ID_S, ID_B	User identification of a seller and a buyer respectively
WM_{ID}	Generated watermark
WM_{DT}	Detected watermark
Simi(*M*,*N*)	Similarity of M and N

B. Registration Protocol

1) Buyer registration. A buyer *B* should register to the *AC* before any purchase. To do this, *B* selects a secret key pair (pk_B, sk_B), and sends the public key pk_B and other information such as user name etc. to the *AC*. The *AC* sends his public key pk_{AC} and a user identification ID_B to the user.

2) Seller registration. A seller *S* also should register to the *AC*. *S* sends the public key pk_S and other information such as user name etc. to the *AC*. The *AC* sends his public key pk_{AC} and a user identification ID_S to the Seller.

3) Digital content registration. When an owner wants to sell her digital product, she sends the digital content, her user identification ID_S, together with a digital certification $Cert_S$ to the *AC*. *AC* then checks the certification $Cert_S$ he receives, if it is valid, he stores a copy of the digital content C_{IDC}, and insert a tuple including *IDC*, ID_S, $Cert_S$, with a time stamp TS_{AC} into system database. That is, (IDC, ID_S, $Cert_S$, TS_{AC}).

AC then feeds back the registered identification IDC to the seller.

C. Watermarking Protocol

In this protocol, all the transactions between the buyers and sellers are coordinated and supervised by the Authentication Center(AC). During each purchase, the three parties engage in the following procedure.

1) *B* sends a purchase request to *S* by providing buyer's ID encrypted by *AC*'s public key, together with the ID of the digital content *IDC*.

$$B \rightarrow S: Epk_{AC}(ID_B), IDC$$

2) *S* forwards the above information to the *AC*:

$$S \rightarrow AC: Epk_{AC}(ID_B), IDC, ID_S$$

3) *AC* checks the registration information by decrypting $Epk_{AC}(ID_B)$, and aborts if *B* is unregistered or invalid ID. Otherwise, *AC* generates a transaction identifier $Tran_{ID}$, sends it to S with $Epk_{AC}(ID_B)$, and *IDC*.

$$AC \rightarrow S: Tran_{ID}, Epk_{AC}(ID_B), IDC$$

4) If *S* wants to abort the transaction, she refuses. Otherwise, *S* send her signature to *AC* to submit her approval to this transaction.

$$S \rightarrow AC: Sign_S(Tran_{ID}, Epk_{AC}(ID_B), IDC, ID_S)$$

5) On receiving the information from *S*. *AC* generates a valid watermark WM_{ID}, embeds it into the content C_{IDC} to get a watermarked copy C'_{IDC}. *AC* then informs *B* to pay *S* the bill.

6) B aborts if he wants to refuse, or pays the bill to *S*.

7) S sends the payment notification to *AC*, and *AC* sends the watermarked copy C'_{IDC} to *B*.

$$AC \rightarrow B: C'_{IDC}$$

8) On receiving the watermarked copy C'_{IDC}, B sends an ACK to AC in a limited time slice.

$$B \rightarrow AC: Sign_B(Tran_{ID}, Epk_{AC}(ID_B), IDC, ID_S)$$

9) AC sends a digital certification to *S* and *B*.

$$AC \rightarrow B,S: Cert(Tran_{ID}, Epk_{AC}(ID_B), IDC, ID_S, WM_{ID}, TS_{AC})$$

Then, AC updates his transaction database by adding the following tuple:

$$(Tran_{ID}, Epk_{AC}(ID_B), IDC, ID_S, WM_{ID}, TS_{AC}) \| Sign_B(Tran_{ID}, Epk_{AC}(ID_B), IDC, ID_S) \| Sign_S(Tran_{ID}, Epk_{AC}(ID_B), IDC, ID_S)$$

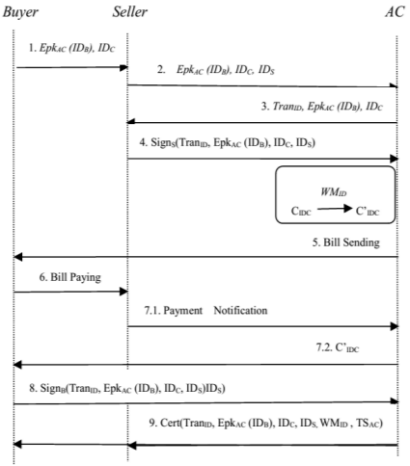

Fig. 1. Detail of watermarking protocol

Details of the proposed watermarking protocol is illustrated in Fig. 1.

D. Traitor Tracing Protocol

If a suspected copy *X*' is found, *S* sends it to the *AC* with the ID of original content. *AC* loads the registered content *X* by the ID, calculates the similarity of *X'* and *X*, *Simi*(*X', X*). If it is under a threshold, then *AC* denies the claim, otherwise he starts a traitor tracing procedure.

To trace a traitor, *AC* first executes the detection algorithm to get the embedded watermark WM_{DT}, if fails, the traitor tracing procedure ends, otherwise, *AC* traverses the local transaction database and locates the relative record by $WM_{DT.}$*AC* can then decrypts the user ID in the pointed record and accuses the buyer according to the user ID.

To prove that a user has illegally distributed a digital content, *AC* and *S* must run the arbitration protocol successfully before a judge.

E. Arbitration Protocol

To prove that a specific buyer *B*' is the leaker of unauthorized content to a judge, *AC* describes the watermark protocol to the judge. Then AC presents the illegal copy and the detected watermark to the judge, together with the corresponding entry of the transaction retrieved from the database.

The judge first verifies similarity of *X*' and *X*, if not passes, he denies the accusation, else, he then checks *B*' signature $Sign_B(Tran_{ID}, Epk_{AC}(ID_B), IDC, ID_S)$ to confirm that *B*' has indeed bought a copy of IDC. Next, the judge launches the watermark detection procedure to get the watermark WM_{DT}, and compares it with the embedded watermark WM_{ID}, if they match, then the judge will approve the accusation, otherwise he will turn down it.

IV. Security Analysis and Discussion

A. Security Analysis

The proposed watermarking protocol takes the following characters.

1) The proposed watermarking protocol is fair to both *S* and *B*. In previous protocols, sellers have partial or full access to the watermark, watermarked digital copy, even a buyer's information, while the buyers usually know nothing about the watermark nor the transaction information. Thus, a privileged seller can easily frame a buyer [7]. This is unfair especially to the buyer in a sense. The proposed watermarking protocol is *AC* centered, namely, all transactions are controlled by *AC*. Unlike previous protocols, the watermark generation, embedding, detecting procedures are solely executed by the *AC*. Both B and S are fully excluded from the watermark procedure, they have equal right in the purchase, so that neither *B* nor *S* has access to the watermark and detecting procedure. On the one hand, the seller doesn't know the exact watermark so she can't maliciously distribute illegal copies and frame the buyer. Thus the "*customer's right problem*" is well solved. On the other hand, the buyer has no idea about the original digital content and the watermark embedded in the copy he purchased, hence, he is unable to remove the watermark.

2) It avoided the "unbinding problem". As described in Ref. [10], the "*unbinding problem"* arises because most of the previously proposed watermarking protocols fail to provide proper mechanisms on binding a chosen watermark to a specific digital content or a specific transaction. Therefore, once the seller discovers a pirated copy, it is possible for her to transplant the watermark embedded in the pirated copy into another copy of a higher-priced digital content to produce made-up piracy so that she can get compensated more. In the proposed watermarking protocol, a unique watermark is embedded into a digital content before it is sold. And this watermark is well kept by AC for later arbitration use. The seller has no access to the watermark or the watermarked copy of the digital content, So that the "*unbinding problem"* is overcome.

3) The proposed watermarking protocol can resist denial attack from a dishonest sellers or buyer. Two aspects of this issue are studied as follows.

Denial of selling. In traditional protocols, the seller may deny her selling of the digital content to a buyer, and accuse related buyer of pirate [14]. In this protocol, if this occurs, *AC* searches his transaction database and get the seller's signature $Sign_S(Tran_{ID}, Epk_{AC}(ID_B), IDC, ID_S)$. By proving the validity of the seller's signature, the dishonesty can be defeated.

Denial of receiving. A dishonest buyer may claim that he has paid the bill, but never get the digital copy. In this case, *AC* retrieves the buyer's signature $Sign_B(Tran_{ID}, Epk_{AC}(ID_B), IDC, ID_S)$ from the transaction database. The buyer's misbehavior can be disclosed by proving the validity of his signature.

4) The proposed watermarking protocol can resist "secondhand watermark attacks". A buyer may modify the copy he bought to some extent and add a second watermark so that he can claim legal ownership of the original copy. According to the proposed protocol, each piece of content is assigned a unique serial number, *IDC*, in the registration phase. And a tuple of $(IDC, ID_S, Cert_S, TS_{AC})$ is added into the system database (see III.B). When ownership disputes on a certain digital content arise, AC recalls the relative records and compares the time stamp, then he can judge that the party who has an earlier time stamp is the legal owner.

5) A buyer's anonymity is well guaranteed.

In the proposed watermarking protocol, a buyer's user ID is encrypted by his public key, so that the basic information of a user is well kept. While in a traitor tracing scenario, the Trusted Third Party(*AC*) can decrypt it and find the very person who pirates. Thus the privacy of the buyer is well kept and the traitor can be traced.

(6) The proposed watermarking protocol is independent to watermark schemes. Unlike some proposed schemes which depend on special watermarking technologies [11], [12], [14], there is no special demand

to watermark schemes in the proposed watermarking protocol. That is, the protocol can be achieved by any watermarking scheme as long as the *AC* likes. This makes the proposed protocol more practicable.

B. Discussion

1) The proposed watermarking protocol is efficient. In the proposed protocol, the seller sends the digital content only once in registration phase. There is no (encrypted) digital content transmission between *AC* and *S*. Thus the communication overhead between *S* and *AC* is reduced especially in the scenario of selling the same content for more than one time. A comparison of information transfer times between Frattolillo's protocol [13] and the proposed one is depicted in Table II. In which, *S-AC* indicates the number of information exchanging between *S and AC*, etc.

TABLE II: COMPARISON OF COMMUNICATION OVERHEAD

	S-AC	B-AC	B-AC
Frattolillo's protocol	6	7	3
Proposed protocol	5	4	3

2) The proposed watermarking protocol is flexible. The purpose of this paper is to propose a secure and fair buyer-seller protocol, not any implementation detail. To concentrate on framework of the proposed protocol, most techniques are abstractly mentioned without giving a certain solution. For example, public key cryptography is used in this paper, however it is never specified. Many cryptography systems are suitable, such as RSA or ECC (Elliptic Curve Cryptography). Another example is the digital certificate scheme, which can be anyone as long as the user likes [10].

V. CONCLUSION

In this paper, we have proposed an *AC* centered buyer-seller protocol. Different to most previous protocols, the watermark embedding, digital content selling, and arbitrating etc. are executed by *AC* in this new proposed protocol. The buyer and the seller are symmetrical clients of a trusted third party (*AC*), neither of them has privilege in the protocol. Thus the proposed protocol is secure, fair, flexible and efficient. Furthermore, the proposed protocol is adapted to most digital media, such as image, audio, video and database etc.

ACKNOWLEDGMENT

This work was supported in part by a grant from China Ministry of education research project of humanities and social science under grant No.11YJCZH021, Natural Science Foundation of Shandong Province of P. R. China under Grant No. ZR2012AL07, ZR2013AM013.

The authors would like to extend their sincere gratitude to the anonymous reviewers for the constructive suggestions, which led to this revised version.

REFERENCES

[1] N. R. Wagner, "Fingerprinting," in *Proc. IEEE Symp. Security and Privacy*, 1983, pp. 18-22.

[2] L. Qiao and K. Nahrstedt, "Watermarking schemes and protocols for protecting rightful ownership and customer's rights," *J. Vis. Commun. Image Representation*, vol. 9, no. 9, pp. 194-210, Sep. 1998.

[3] A. Rial, J. Balasch, and B. Preneel, "A privacy-preserving buyer-seller watermarking protocol based on priced oblivious transfer," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 202-212, Jan. 2011.

[4] Y. W. Peng, C. J. Wang, Y. Fang, and W. B. Li, "Anonymous watermarking protocol for vector spatial data," in *Proc. International Conference on Computer Science & Service System*, 2012, pp. 2095-2098.

[5] B. Terelius, "Towards transferable watermarks in buyer-seller watermarking protocols," in *Proc. IEEE International Workshop on Information Forensics and Security*, 2013, pp. 197-202.

[6] M. K. N. Haji and Z. Eslami, "An efficient buyer-seller watermarking protocol based on proxy signatures," in *Proc. Information Security and Cryptology Conf.*, 2011, pp. 73-78.

[7] N. Memon and P. Wang, "A buyer-seller watermarking protocol," *IEEE Trans. Image Process.*, vol. 10, no. 4, pp. 643–649, Apr. 2001.

[8] T. Bianchi and A. Piva, "TTP-Free asymmetric fingerprinting based on client side embedding," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1557-1568, Oct. 2014.

[9] J. G. Choi and J. H. Park, "A generalization of an anonymous buyer-seller watermarking protocol and its application to mobile communications," in *Proc. 3rd Int. Workshop Digital Watermarking, ser. Lect. Notes Comput. Sci. Berlin, Germany: Springer*, 2004, vol. 3304, pp. 232–243.

[10] C. Lei, P. Yu, P. Tsai, and M. Chan, "An efficient and anonymous buyer-seller watermarking protocol," *IEEE Trans.* Image *Process.*, vol. 10, no. 4, pp. 643–649, Apr. 2004.

[11] T. R. Srinath, S. Kella, and M. J. enamani, "A new secure protocol for multi-attribute multi-round e-reverse auction using online trusted third party," in *Proc. Emerging Applications of Information Technology International Conf*., 2011, pp. 149-152.

[12] Y. Zhao, A. Zhang, and S. N. Lu, "Group fingerprinting communication protocols for digital wholesale and retail in E-commerce," in *Proc. Informatics and Applications International Conf*, Sept. 23-25, 2013, pp. 143-146.

[13] F. Frattolillo, "Watermarking protocol for web context," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 350–363, Sep. 2007.

[14] S. Katzenbeisser, A. Lemma, M. U. Celik, *et al*., "A buyer-seller watermarking protocol based on secure embedding," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 4, pp. 783-786, Dec. 2008.

Xinchun Cui was born in Shandong Province, P. R. China, in 1971. He received the B.S. Degree from Shandong Normal University, Ji'nan, in 1995, the M.S. degree from Shanghai Normal University, Shanghai, in 2002, and the Ph.D. Degree from Nanjing University of Aeronautics and Astronautics, all in computer science. He is currently a professor with the School of Information Science and Engineering of Qufu Normal University (Rizhao Campus). His research interests include digital watermarking, signal processing, and information security.

Gang Sheng was born in Shandong Province, P. R. China, in 1978. He received the B.S. Degree from Qufu Normal University, Qufu, in 2000, M.S. degree and the Ph.D. from Northeast University, Shenyang, in 2005, and 2015. He is currently a Lecturer with the School of Management of Qufu Normal University (Rizhao Campus). His research interests include digital watermarking, information security.

Fengyin Li was born in Shandong Province, P. R. China, in 1974. She received the B.S. Degree, M.S. degree and the Ph.D. degree in computer science from Shandong Normal University, Ji'nan, in 1998, 2010, and 2014 respectively. She is currently a vice professor with the School of Information Science and Engineering of Qufu Normal University (Rizhao Campus). Her main research interests are digital signature, information security etc.

Xiaowu Liu was born in Shandong Province, P. R. China, in 1976. He received the M.Sc and Ph.D degrees in computer science from the Harbin Engineering University in 2005 and 2009 respectively. He is currently a vice professor with the School of Management of Qufu Norml University (Rizhao Campus), and an advanced expert instructor of Cisco Networking Academy. His current research focuses on network security, cognitive computing and information fusion.