A Verifiable and Traceable Secondhand Digital Media Market Protocol

Chin-Ling Chen[1] and Chin-Chang Chen[2]
[1] Dept. of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung, Taiwan 41349, ROC.
[e-mail: clc@mail.cyut.edu.tw]
[2] Dept. of Computer Science and Information Engineering, National Chung Hsing University, Taichung, Taiwan 402, ROC.
[e-mail: u32131@yungshingroup.com]

Received July 19, 2010; revised September 5, 2010; accepted October 15, 2010; published August 29, 2011

Abstract

As used product transactions are currently on the rise, the demand for transactions of secondhand digital content will grow in the future; thus, learning to make secure transactions while avoiding cyber attacks becomes an important issue. In this paper, we combine the new buyer's secret key, the new buyer's watermark to embed in resold digital content, and the reseller's encrypted watermark, which can prove legal ownership of the reseller. Using the privacy homomorphism property of RSA and exponential calculus, the original seller of digital content can verify the legality of the reseller and the new buyer. We also reduced the load of encryption/decryption digital content using a partial encryption/decryption algorithm to make our protocol more efficient and practical. In the proposed protocol, the seller is not able to conduct piracy and easily frame any other innocent secondhand buyer when a case of piracy is found. In fact, piracy can be clearly traced using the privacy homomorphism property of RSA and the embedded watermark mechanism. Further, in the proposed protocol, the seller himself can trace the piracy using exponential calculus. Since it is unnecessary to trust third party participation, the conspiracy problem is resolved and the new buyer is not required to participate in the dispute. Moreover, the seller, reseller and new buyer can simultaneously benefit from the secondhand transaction.

Keywords: Buyer-reseller, copyright protection, digital watermark, authentication, digital content

DOI: 10.3837/tiis.2011.08.007

1. Introduction

With the increasing growth and popularity of digital technology and the Internet, digital media (such as music, images, movies, etc.) have been widely adopted. Similarly, the demand for secondhand digital media is growing. Like digital content transactions, reselling digital media increases the risk of unauthorized digital content distribution; therefore, the protection of the ownership and copyright of digital content is an imperative issue for secondhand transactions.

After Memon and Wang [1] used the watermark and the privacy homomorphism to protect seller's copyright and buyer's ownership in 2001, many protocols were proposed to solve the numerous security problems in firsthand digital content transactions. However, only a few protocols mentioned secondhand digital content transactions. In the secondhand market, the pricing of used digital content depends on its popularity, not its depreciation. Since used digital content is just as functional as new digital content, in the proposed protocol, all parties involved in the secondhand transaction can benefit. The buyer can obtain digital content at a lower price; the reseller can profit from it, and the original seller can profit from the fee that is charged for providing an ownership transfer service.

In our protocol, the seller secretly inserts two unique digital watermarks into the resold digital content without causing degradation for the purpose of copyright protection. Once piracy is found in the market, the original seller can extract embedded watermarks from the replica to find the pirated content. For maintaining the legality of piracy tracing, the watermark must be protected from the seller during the transaction. For watermark security, our buyer-reseller protocol adopts the private homomorphism property of RSA **(**Rivest; Shamir; Adleman) as a tool to insert watermarks into digital content. According to the private homomorphism property, the new buyer first encrypts his secret watermark with his public key. In order to embed the new buyer's watermark in the digital content, the seller must use the same public key to encrypt the digital content for trade so the seller can embed the buyer's watermark into the digital content under the encryption domain. There are two purposes of the private homomorphism property in the secondhand digital media market protocol. The first is to eliminate the possibility of a malicious seller framing an innocent buyer with a counterfeit, and the second is to trace the illegal distributors through replicas found in the market.

To avoid the possibility of the seller transplanting the watermark embedded in the pirated copy into other higher-priced digital content and framing the new buyer, we use a novel way to combine the new buyer's secret key, watermark, and the reseller's encryption watermark. The seller cannot frame the new buyer or the reseller unless he or she can obtain the exact secret key.

An untrustworthy third party may collude with a malicious seller to fabricate piracy and frame an innocent buyer; or they may collude with a malicious buyer to confuse the trace of piracy by faking the watermark, which would cause conspiracy problems. Considering this, a secondhand digital media market protocol without any third party participation is more secure and practical during the transaction; moreover, it is closer to the original product. The only drawback of the secondhand digital media market protocol without a Trusted Third Party (TTP) is only new buyers can prove the authenticity of the watermark themselves. Therefore, the new buyer has to participate in disputation to prove his or her innocence. To solve these

problems, we propose a verifiable and traceable secondhand digital media market protocol using the privacy homomorphism property of RSA and the embedded watermark mechanism. The proposed scheme not only can guarantee the privacy of the buyer's watermark but also avoid the TTP's participation during the transaction. It can prevent the known attacks of the buyer-reseller watermark protocol and encapsulate security problem solutions.

The rest of this paper is organized as follows: Section 2, briefly reviews the buyer-reseller watermarking literature. Section 3 introduces two important preliminaries in the buyer-reseller watermark protocol are introduced. Section 4 provides detailed descriptions of the proposed protocol used to achieve our goals. Section 5 discusses relevant security issues in secondhand digital media market and compares it to previous schemes. Section 6 concludes our proposal.

2. Literatures review

The core mechanism of the new secondhand digital media market is the seller inserts the new buyer's watermark and the reseller's encryption watermark into the digital content without obtaining any information about the watermark. The seller cannot be granted access to the digital content after the watermark has been embedded. The embedded watermark can be extracted from the pirated copy for evidence to trace the pirate.

Despite the many buyer-seller watermark protocols trying to use asymmetric [1][2][3][4][5][6][7][8] or symmetric encryption [9] skill to protect buyer or seller's right in digital content trade since 2001, there have been very few proposals for secondhand digital media market protocol [10][11][12].The earliest research on secondhand digital media market protocol was proposed by Cheung and Curreem [10] in 2002. Their proposal tried to protect the new buyer's rights based on the buyer-seller watermarking protocol proposed by Memon and Wong [1]. Through the privacy homomorphism property, the new buyer provides the seller with an encrypted watermark and the digital content obtained from the reseller to defend the interests of buyers against sellers' unethical distribution of watermarked contents.

In 2005, Chen et al. [11] showed the Cheung and Curreem's scheme suffers from the seller cheating and reseller cheating problems. Cheung and Curreem's scheme was not secure and an improvement was proposed to further protect the privacy of both buyers and resellers. But Chen et al.'s scheme still had some security issues that required solving. In 2008, Liu et al. [12] also proposed a secure buyer-reseller watermarking protocol; by keeping the entire transaction under an encryption domain, the buyer's watermark and the digital content remain protected from the original seller's attack during the transaction. The proposed protocol can effectively prevent collusion attacks and man-in-the-middle attack if the third party is not trusted. Also, the buyer-reseller watermarking protocol only needs the seller to provide a transfer certificate and encryption-decryption service to support the second-hand transaction and it can also trace the original dishonest buyer. However, Liu et al.'s weakness is they apply a double encryption method, with zero knowledge verification techniques placed into the scheme and three watermarks need to be embedded into the digital content.Thus, the computation requirements are too great.

In our view, in addition to computation cost, a well designed secondhand digital media market protocol must have the same security level as a buyer-seller watermark protocol. All security issues mentioned in a buyer-seller watermarking protocol should also be resolved in a secondhand digital media market protocol. These important issues including the following problems:

(1) New buyer's right problem: When a new buyer's watermark is solely inserted by the

original seller, the original seller may benefit from framing an innocent new buyer.

(2) The unbinding problem: The seller may fabricate piracy by transplanting the new buyer's watermark into other digital content.

(3) The piracy trace problem: When piracy is found, it should be traceable and identifiable by the original seller.

(4) The conspiracy problem: Malicious parties may collude with one another to frame an innocent party or to confound the traceability by faking or removing the watermark.

(5) New buyer's participation in the dispute resolution problem: The arbitrator cannot resolve disputes unless the new buyer reveals his identity or private key.

(6) The man-in-the-middle attack problem: A malicious third party can attack if either party discloses their secret during the transaction.

(7) The anonymity problem: The buyer should remain anonymous during the transaction until he is judged to be guilty.

In this paper, we try to propose an efficient, verifiable and traceable secondhand digital media market protocol to satisfy the mentioned requirements.

3. Preliminary

3.1 Privacy homomorphism

In 1978, Rivest et al. [13] proposed the technique of privacy homomorphism to act as a tool for processing encrypted data. It was first introduced by Memon and Wong in their secondhand digital media market protocol to settle the customer's rights problem and piracy tracing problem in 2001. Privacy homomorphism allows us to perform certain designated operations on encryption data without disclosing the original data. Most secondhand digital media market protocols adopted the public key infrastructure (PKI) cryptosystem to protect both the new buyer's and the seller's rights. The RSA public key cryptosystem is a privacy homomorphism, with respect to the multiplication operation and the basis of RSA privacy homomorphism. It is described as follows:

$$\begin{aligned} & E_{pk}(A) \times E_{pk}(B) \\ & \equiv (A^e \times B^e) \bmod n \\ & \equiv (AB)^e \bmod n \\ & \equiv E_{pk}(AB) \bmod n \end{aligned} \tag{1}$$

Where $E_{pk}(.)$ is an asymmetric encryption algorithm with the public key e, and the modulus $n=pq$, p and q are two (odd) prime numbers. For A and B, whether we perform multiplication before encryption or perform encryption before multiplication is irrelevant.

3.2 Watermark insertion

Two watermark insertion methods may be used in the new secondhand digital media market protocol to protect digital ownership or copyright. One is the spatial domain method and the other is the frequency domain method. We use an image as an example. With the spatial domain method, a watermark is inserted into the image by directly modifying the least significant bit (LSB) of some pixel values in the image. The advantage of the spatial domain

method is it has faster computation. The disadvantage is it can barely withstand image attacks such as cutting, compressing, zooming and rotating; it is also less tolerant to noise. In the frequency domain method, the image is transformed into frequency domain coefficients by some transformations, such as the Discrete Cosine Transformation (DCT), the Fast Fourier Transformation (FFT) and the Discrete Wavelet Transformation (DWT) [14], prior to embedding the watermark into the image. This method is more complex and slower than the spatial domain method; however, the frequency domain method is more secure and tolerant to noise than the spatial domain method. The frequency domain method is much more suitable for the secondhand digital media market protocol than the spatial domain method.

For the watermark insertion operation, the digital content to be sold is regarded as a vector of features χ, where $\chi = \{\chi_1, \chi_2, ..., \chi_n\}$. And the watermark to be inserted is regarded as a vector of features ω, where $\omega = \{\omega_1, \omega_2, ..., \omega_m\}$. The watermarking scheme is regarded as linear and the insertion operation can be represented as the computation of

$$\chi' = \chi \otimes \omega = \{\chi_1 \otimes \omega_1, \chi_2 \otimes \omega_2, \chi_3 \otimes \omega_3, ..., \chi_m \otimes \omega_m\} \tag{2}$$

where $\otimes$ is the watermark insertion algorithm. The watermark insertion operation is used in the secondhand digital media market protocol as an arbitration basis to protect the digital ownership and copyright.

4. The proposed protocol

The proposed protocol is based on a robust spread-spectrum watermarking technique originally proposed by Cox et al. [15] along with the RSA cryptosystem to embed the new buyer's watermark into the digital content. All transaction information between the new buyer and the seller is encrypted before sending. In this paper, the new buyer's unique private key will be separated into a specific watermark and the reseller's encrypted watermark information. Since the new buyer's one-time private key is generated based on an RSA cryptosystem, the security of the watermark and the reseller's encrypted watermark information will be held and verified. Moreover, through the privacy homomorphism property of RSA and designed exponential calculus, the seller can verify the authenticity of the new buyer's watermark and the reseller's encrypted watermark without decrypting them. Therefore, our proposed protocol can eliminate the requirement of a third party, prevent the new buyer from participating in the dispute resolution, and verify the ownership of the reseller simultaneously. The transaction flow is depicted as in **Fig. 1**.

The overview of our scheme is described as follows.

1. New Buyer→ CA: The new buyer applies for Certificate Authority (CA) of an anonymous digital certificate.
2. CA→ New Buyer: The CA issues an anonymous digital certificate to the new buyer.
3. New Buyer→ Reseller: The new buyer sends a purchase request to the reseller.
4. Reseller→ New Buyer: The reseller issues reselling information to the new buyer.
5. New Buyer→ Original Seller: The new buyer sends a purchase and verification information to the original seller.
6. Original seller→ New Buyer: The original seller issues digital content.

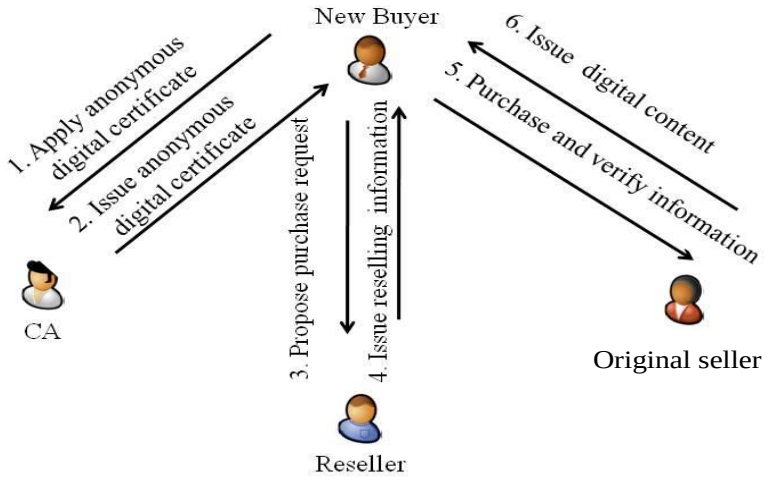

Fig. 1. Transaction flow of our protocol

There are six phases in our proposed scheme, i.e., phases of registration, initiation, watermark generation, ownership and watermark verification, watermark insertion and piracy dispute resolution, with detailed descriptions presented in the following subsections. In addition, the notation used through this paper is shown as follows:

ID_N : identity of the new buyer

$Cert_N$: anonymous digital certificate issued to the new buyer which conforms the X.509 format

$\|$: concatenation operation

M : digital content for reselling, where $M = M_1 \| M_2 \| ... \| M_n$

M_i : the i-th data block of digital content, where $1 \le i \le n$

M_{desc} : description of digital content

ε : new buyer's watermark

$c\varepsilon$: cyphertext of the new buyer's watermark

w : reseller's watermark

cw : cyphertext of the reseller's watermark

$Y \stackrel{?}{=} Z$: compare whether Y is equal to Z

σ : random factor of digital content chosen by the original seller

$s(.)$: encrypt block selection algorithm

pk_B / sk_B : reseller's public/private key pair

$pk_B^{\ i} / sk_B^{\ i}$: reseller's one-time public/private key pair

pk_N / sk_N : new buyer's public/ private key pair

$pk_N^{\ i} / sk_N^{\ i}$: new buyer's one-time public/ private key pair

pk_S / sk_S : original seller's public/ private key pair

$S_{sk_X}(m)$: sign message m with X's secret key

$V_{pk_X}(m)$: verify message m with X's public key

$E_{pk_X}(m)$: encrypt message m with X's public key

$D_{sk_X}(m)$: decrypt message m with X's secret key

RI_{NB} : reselling information, where $RI_{NB} = (Cert_N, cw, M_{desc})$

$Sign_R$: signature of RI_{NB} signed by the new buyer , where $Sign_R = (S_{sk_N{}^i}(S_{sk_B}(RI_{NB}))$

$\otimes$: watermark insertion algorithm

$\odot$: watermark extraction algorithm

4.1 Registration phase

The new buyer applies for an anonymous digital certificate as identification, which is issued by the certification authority, while it is assumed the communication between the two parties is secure. For example, the Secure Socket Layer (SSL) is involved in our proposed scheme to prevent any tampering. As illustraed in **Fig. 2**, the two-step registration scenario can be described as follows:

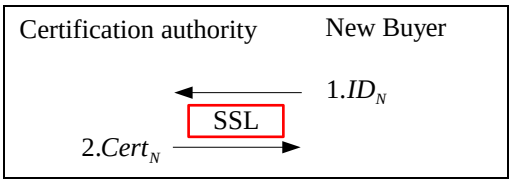

Fig. 2. Registration protocol

1. The new buyer proposes his or her identity ID_N to the Certification Authority;
2. The Certification Authority issues an anonymous digital certificate $Cert_N$ to the new buyer after ID_N is verified.

4.2 Initiation phase

The new buyer sends the anonymous digital certificate as a purchase request to the reseller. After receiving the request, the reseller prepares the related purchase information for acquiring the new buyer's confirmation. The scenario shown in **Fig. 3** can be stated as below:

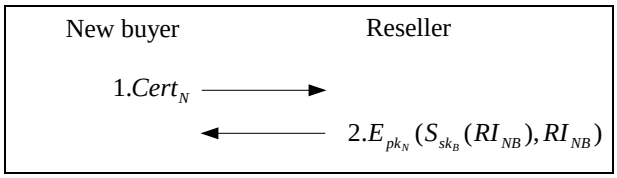

Fig. 3. Initiation protocol

1. The new buyer sends the anonymous digital certificate $Cert_N$ to the reseller as a purchase request;
2. After receiving the new buyer's purchase request, the $Cert_N$, cw and M_{desc} are combined and signed by the reseller to form the resell information RI_{NB}, where $RI_{NB} = (Cert_N, cw, M_{desc})$. Then reseller sends this signed RI_{NB} to the new buyer for further confirmation.

4.3 Watermark generation phase

The new buyer verifies the authenticity of the received reselling information. If the verification result is positive, the new buyer will generate a secret watermark and a one-time public/private key pair for this transaction and sign the reselling information with a private key. Then, the new buyer will send the order information to the original seller. The scenario is depicted in **Fig. 4** can be described in the following five steps.

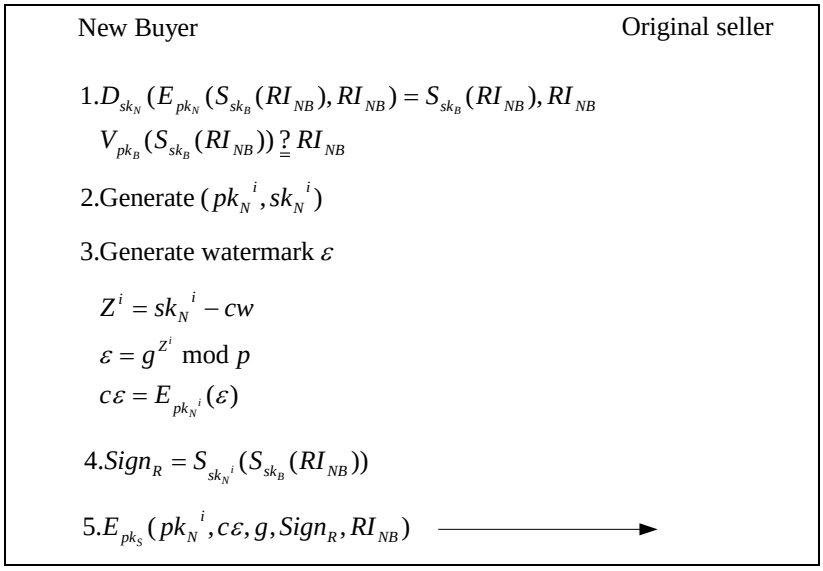

Fig. 4. Watermark generation protocol

1. After decrypting the reselling information sent from the reseller, the new buyer verifies the authenticity of $S_{sk_B}(RI_{NB})$ through the reseller's public key pk_B and RI_{NB} by the following sub-procedures,

$$D_{sk_N}(E_{pk_N}(S_{sk_B}(RI_{NB}), RI_{NB})) = S_{sk_B}(RI_{NB}), RI_{NB} \tag{3}$$

and

$$V_{pk_B}(S_{sk_B}(RI_{NB})) \stackrel{?}{=} RI_{NB}; \tag{4}$$

2. After verifying RI_{NB}, the new buyer generates a one-time public-private key pair $pk_N{}^i / sk_N{}^i$ for this transaction;
3. The new buyer generates an encrypted watermark $c\varepsilon$ for this transaction by the following operations,

$$Z^i = sk_N{}^i - cw, \tag{5}$$

$$\varepsilon = g^{Z^i} \bmod n, \tag{6}$$

$$c\varepsilon = E_{pk_N{}^i}(\varepsilon); \tag{7}$$

4. The new buyer signs the signature $S_{sk_B}(RI_{NB})$ using the one-time private key $sk_N{}^i$ to generate a dual signature $Sign_R$, where

$$Sign_R = (S_{sk_N{}^i}(S_{sk_B}(RI_{NB})); \tag{8}$$

5. After $c\varepsilon$ is generated, the new buyer encrypts $(pk_N{}^i, c\varepsilon, g, Sign_R, RI_{NB})$ with the original seller's public key pk_S, and then sends all the encrypted information

$E_{pks}(pk_N{}^i, c\varepsilon, g, Sign_R, RI_{NB})$ to the original seller.

4.4 Ownership and watermark verification phase

After charging the proper service fees, the original seller decrypts and verifies the authenticity of the encrypted order information; then the original seller searches the sale database with the reseller's encrypted watermark. If there is a matching record found in the sale database, the original seller then executes the new buyer's watermark verification using a predefined formula. The whole scenario shown in **Fig. 5** can be summarized as the following three steps:

Original seller

1. $D_{sk_S}(E_{pk_S}(pk_N{}^i, c\varepsilon, g, Sign_R, RI_{NB}) = pk_N{}^i, c\varepsilon, g, Sign_R, RI_{NB}$

2. $V_{pk_N{}^i}(V_{pk_B}(Sign_R)) \stackrel{?}{=} RI_{NB}$

   Search transaction record according to $c\varepsilon$

3. *Verify* $c\varepsilon \times E_{pk_N{}^i}(g^{cw}) \stackrel{?}{=} g$

Fig. 5. Owership and watermark verification protocol

1. The original seller uses the private key sk_S to decrypt the encrypted order information sent from the new buyer, and then verifies $Sign_R$ with pk_B and $pk_N{}^i$ by

$$D_{sk_S}(E_{pk_S}(pk_N{}^i, c\varepsilon, g, Sign_R, RI_{NB})) = (pk_N{}^i, c\varepsilon, g, Sign_R, RI_{NB}) \tag{9}$$

and

$$V_{pk_N{}^i}(V_{pk_B}(Sign_R)) = RI_{NB}; \tag{10}$$

2. The original seller searches the sale database according to the reseller's encrypted watermark cw. If cw cannot be found in the database, the transaction is rejected;
3. The original seller then verifies the authenticity of the new buyer's encrypted watermark $c\varepsilon$ using the following definition, i.e.,

$$\begin{aligned} & c\varepsilon \times E_{pk_N{}^i}(g^{cw}) \\ &= E_{pk_N{}^i}(\varepsilon) \times E_{pk_N{}^i}(g^{cw}) \\ &= E_{pk_N{}^i}(\varepsilon \times g^{cw}) \\ &= E_{pk_N{}^i}(g^{Z^i} \times g^{cw}) \\ &= E_{pk_N{}^i}(g^{Z^i + cw}) \\ &= E_{pk_N{}^i}(g^{sk_N{}^i}) \\ &= E_{pk_N{}^i}(D_{sk_N{}^i}(g)) = \stackrel{?}{=} g; \end{aligned} \tag{11}$$

If Eq. (11) holds, the original seller accepts the ownership transfer request; otherwise the request is rejected.

4.5 Watermark insertion phase

The original seller inserts their encrypted watermark into the digital content under encryption, then sends the encrypted digital content to the new buyer. For granting higher efficiency, partial encryption is adopted to replace all of the encryption in the watermark insertion phase.

The original seller divides the digital content into blocks. Then, he or she encrypts and inserts the new buyer's watermark and the reseller's encrypted watermark into some of the blocks according to a predefined algorithm. The scenario illustrated in **Fig. 6** and **Fig. 7** can be described as follows:

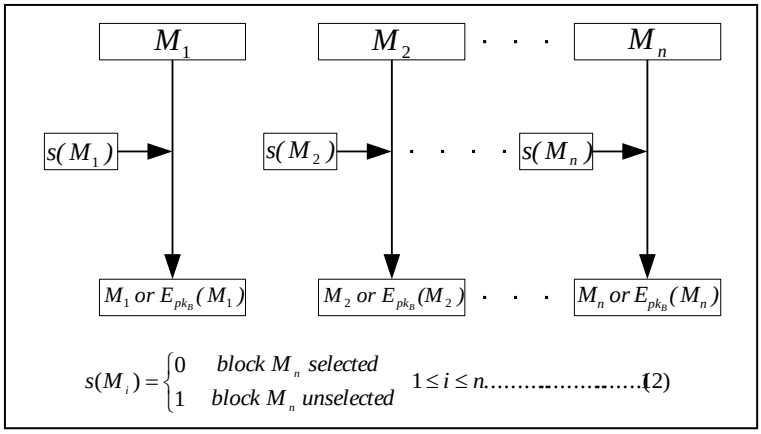

Fig. 6. Encrypt blocks selection algorithm

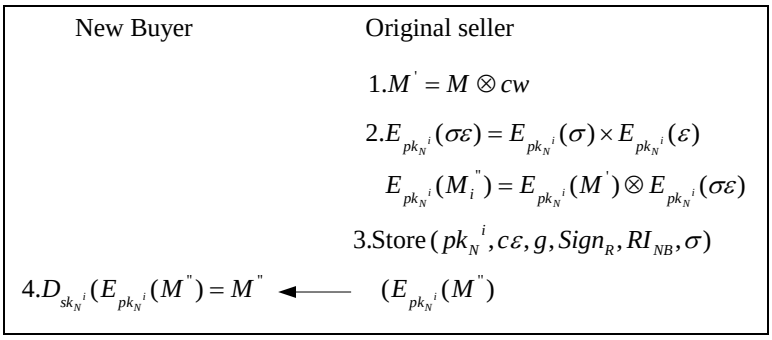

Fig. 7. Watermark insertion protocol

1. The original seller inserts cw into the digital content M to obtain M'. Once piracy is found in the market, the cw can act as an index for the original seller to search the resale database and to retrieve the reselling information, where
$$M' = M \otimes cw; \quad (12)$$
2. To prevent new buyer extracting the watermark from the original digital content, the new buyer's encryption watermark has to be randomized through random factor σ. The original seller embeds the randomized watermark $\sigma\varepsilon$ into the M''. According to the private homomorphism property of RSA, the watermark ε can be embedded into the digital content M as follows.

$$\begin{aligned} & E_{pk_N{}^i}(M') \otimes c\varepsilon \times E_{pk_N{}^i}(\sigma) \\ &= E_{pk_N{}^i}(M') \otimes E_{pk_N{}^i}(\varepsilon) \times E_{pk_N{}^i}(\sigma) \\ &= E_{pk_N{}^i}(M') \otimes E_{pk_N{}^i}(\sigma\varepsilon) \\ &= E_{pk_N{}^i}(M' \otimes \sigma\varepsilon) \\ &= E_{pk_N{}^i}(M \otimes cw \otimes \sigma\varepsilon) \end{aligned}$$

$$= E_{pk_N{}^i}(M'') \tag{13}$$

3. The original seller saves the resale record $(pk_N{}^i, c\varepsilon, g, Sign_R, RI_{NB}, \sigma)$ to the resale database and then sends the encrypted digital content $E_{pk_N{}^i}(M'')$ to the new buyer.
4. The new buyer decrypts $E_{pk_N{}^i}(M'')$ with a one-time private key $sk_N{}^i$ and retrieves the digital content M_R'', where ε and cw were embedded in the digital content, and

$$D_{sk_N{}^i}(E_{pk_N{}^i}(M'')) = M''. \tag{14}$$

4.6 Piracy dispute resolution phase

If a pirated copy is found in the market, the original seller can use the watermark extract algorithm to restore the correct embedded watermark. As mentioned previously, the reseller's encrypted watermark can be used as an index to search the resale database for a corresponding record till the watermark can successfully be extracted from the digital content. In other words, if the matching record is found in the resale database, the original seller can send the record along with the pirated copy and the watermark extract algorithm to the one asking for arbitration, while the specific arbiter can determine the outcome without requiring any assistance from the new buyer during arbitration. The scenario presented by **Fig. 8** can be described in the following six steps.

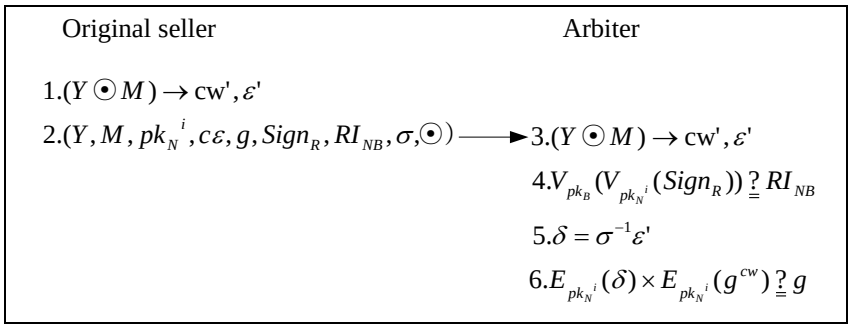

Fig. 8. Piracy dispute resolution protocol

1. When the original seller finds a pirated copy of M'', say Y, in the market, he or she uses the watermark extract algorithm $\odot$ to extract the encrypted reseller's watermark cw' and the new buyer's watermark ε' from Y, by the relations below,

$$(\mathrm{Y} \odot M) \rightarrow (cw', \varepsilon'); \tag{15}$$

note: If ε' and cw' cannot be successfully extracted from Y, this pirated copy is not processed and sold by the seller. In other words, if they can be extracted by the original seller using the watermark extract algorithm $\odot$, the seller can then use cw' as an index to search the resale database for the matching record;
2. After finding the resale record from the resale database, the original seller requests arbitration by sending the record $(pk_N{}^i, c\varepsilon, g, Sign_R, RI_{NB}, \sigma)$, the illegal distribution Y and the watermark extract algorithm $\odot$ to the arbiter;
3. When receiving an arbitration request, the arbiter tries to extract ε' and cw' from the illegal distribution Y through the watermark extract algorithm $\odot$. If the watermarks cannot be obtained from Y, the case will be terminated; otherwise, the arbiter will proceed with the watermark verification procedure;

4. The arbiter verifies the authenticity of the signature $Sign_R$ by

$$V_{pk_B{}^i}(V_{pk_B}(Sign_R)) \stackrel{?}{=} (Cert_N, cw, M_{desc}). \tag{16}$$

4.1 If the illegal copy Y differs from the description of M_{desc}, the following procedures will be terminated.

4.2 If Y conforms with M_{desc}, the arbiter then verifies the authenticity of cw.

4.3 If cw' and cw differ the following procedures will be terminated; otherwise, the arbiter proceeds to verify the new buyer's watermark;

5. The arbiter applies a random factor σ to restore the new buyer's watermark;

6. In the verification process of the new buyer's watermark, the arbiter restores the embedded watermark δ from ε' using the new buyer's one-time public key $pk_N{}^i$ to obtain an encrypted watermark $c\delta$ first, where.

$$c\delta = E_{pk_N{}^i}(\delta). \tag{17}$$

Following step 6, the arbiter determined whether the buyer is guilty through the following definition, i.e.,.

$$\begin{cases} c\delta \times E_{pkN^i}(g^{cw}) = g & \text{Buyer is guilty} \\ c\delta \times E_{pkN^i}(g^{cw}) \neq g & \text{Buyer is innocence} \end{cases} \tag{18}$$

6.1 If the result is not equal to *g,* the illegal copy was not leaked from the new buyer whom the original seller had accused.

6.2 If the result is equal to g, the arbiter can determine the new buyer is guilty. The arbiter sends an anonymous digital certificate $Cert_N$ to the certification authority and asks for the new buyer's true identification only if the new buyer is determined guilty. In other words, actual identification will not be exposed if the new buyer is found to be innocent. **Fig. 9** depicts the arbitration flow:

5. Discussions

The nature of digital content and the scenario between buyer-seller watermark protocol and buyer-reseller watermark protocol is extremely similar. In this section, we use these similar requirements to discuss the security issues of the secondhand digital media market protocol and explain how to solve these problems.

5.1 New buyer's right problem

The key to solving this problem is to keep the new buyer's watermark under encryption during the secondhand transaction. The original seller can only insert watermarks into the digital content using the private homomorphism property; thus, the new buyer's watermark can be inserted into digital content by the original seller without disclosing it.

In the proposed protocol, we use the encrypted watermark $c\varepsilon$ produced by the encryption algorithm $E_{pk_N{}^i}(.)$ as a buyer's identity in the transaction. The original seller cannot extract the new buyer's watermark ε from $c\varepsilon$ without possessing the new buyer's one-time private key $sk_N{}^i$. According to the private homomorphism property, the original seller encrypts the digital content M' using a one-time public key $pk_N{}^i$ before embedding the encrypted

watermark $c\varepsilon$ into it. Thus, the watermark ε can be inserted into digital content M' with respect to the multiplication operation in the RSA cryptosystem, as follows:

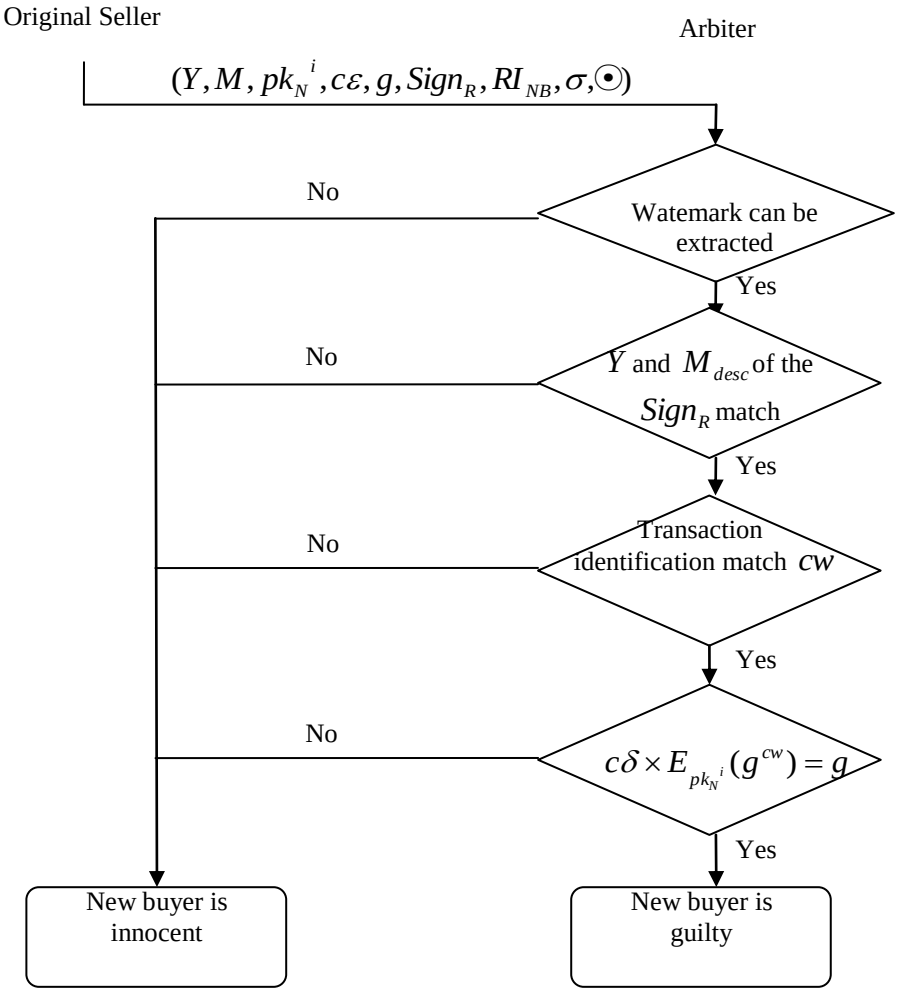

Fig. 9. The arbitration flow

$$
\begin{aligned}
& E_{pk_N{}^i}(M') \otimes c\varepsilon \\
&= E_{pk_N{}^i}(M') \otimes E_{pk_N{}^i}(\varepsilon) \\
&= E_{pk_N{}^i}(M' \otimes \varepsilon) \\
&= E_{pk_N{}^i}(M \otimes cw \otimes \varepsilon) \\
&= E_{pk_N{}^i}(M'')
\end{aligned}
$$

This way, the proposed scheme can prevent the malicious seller from obtaining the new buyer's watermark and embedding it into another duplicate. In the proposed protocol, the security of the watermark, which is embedded into the digital content, can be protected. Besides, the resell content will be encrypted by the new buyer's public key during the watermark insertion phase and the reseller can not access this content anymore since he or she doesn't have the corresponding key.

5.2 Reseller's right problem

Our protocol, we use cw as an identification during the secondhand transaction. The original seller can't decipher the $c\varepsilon$ since he or she doesn't have the decryption key $sk_B{}^i$. And in our protocol, the reseller offers his or her encrypted watermark cw and the description of digital content M_{desc}. This can legally prove the reseller ownership of digital content without revealing the reseller's watermark w. So, the reseller's right can be protected.

5.3 Unbinding problem

The key to solving this problem is to establish a link between the new buyer's watermark and the digital content, i to prevent a malicious seller from obtaining the watermark ε and framing the new buyer by inserting this watermark into other higher-priced digital content.

In the proposed scheme, we link the watermark ε and the reseller's encrypted watermark cw with the following formulas.

$$Z^i = sk_N{}^i - cw$$

$$\varepsilon = g^{Z^i} \bmod n$$

$$c\varepsilon = E_{pk_N{}^i}(\varepsilon)$$

Then we use the reseller's private key sk_B and the buyer's one-time private key $sk_N{}^i$ to sign the resale information $RI_{NB} = (Cert_N, cw, M_{desc})$ and obtain a dual signature $Sign_R$, as follows:

$$Sign_R = (S_{sk_N{}^i}(S_{sk_B}(RI_{NB}))$$

Here, the reseller's encrypted watermark cw and the digital content description information M_{desc} is linked by $Sign_R$. Through the new buyer's watermark generation formula and dual signature, we can firmly link the new buyer's watermark, the reseller's encrypted watermark and the digital content description information to defeat the unbind attack.

5.4 Piracy tracing problem

Because only the buyer has the $sk_N{}^i$ key to decrypt the encrypted digital content, we insert the watermark ε into the digital content M' along with a privacy homomorphism with respect to the multiplication operation under the RSA cryptosystem. To protect the buyer's rights, the new buyer's watermark is encrypted by a one-time public key $pk_N{}^i$ before sending it to the seller, as shown below:

$$c\varepsilon = E_{pk_N}{}^i(\varepsilon)$$

Prior to inserting the watermark ε into the digital content $M_R{}'$, the original seller must encrypt this digital content with the buyer's one-time public key $pk_N{}^i$; then he or she must insert the watermark into the encrypted digital content along with a privacy homomorphism into the RSA cryptosystem as discussed in subsection 3.1.

Here, we can see the original seller can no longer know the digital content once the new buyer's watermark is embedded under the encryption domain. The new buyer is the only one who can access the encrypted digital content $E_{pk_N}{}^i(M'')$. If there is suspicious digital content found in the market, the arbiter can easily determine its real distributor through the embedded watermark.

5.5 Conspiracy problem

Like the buyer-seller watermark protocol, the most effective solution for the conspiracy problem is to eliminate the demand of the TTP from the buyer-reseller watermark protocol. The proposed protocol uses the novel watermark generation mechanism and the verification formulas to eliminate the demand of TTP; therefore, the conspiracy problem can be avoided.

5.6 Buyer's participation in the dispute resolution problem

In our protocol, the new buyer's watermark ε' is extracted from the pirated copy Y, which can be verified through a predefined formula as follows:

$$\begin{aligned} & c\delta \times E_{pk_N{}^i}(g^{cw}) \\ &= E_{pk_N{}^i}(\varepsilon') \times E_{pk_N{}^i}(g^{cw}) \\ &= E_{pk_N{}^i}(\varepsilon' \times g^{cw}) \\ &= E_{pk_N{}^i}(g^{z^i} \times g^{cw}) \\ &= E_{pk_N{}^i}(g^{sk_N{}^i{}'}) \\ &= E_{pk_N{}^i}(D_{sk_N{}^i}(g)) \stackrel{?}{=} g \end{aligned}$$

Using this formula, the arbiter can verify whether the piracy had been leaked from the new buyer without the new buyer's assistance. It is also unnecessary to decrypt the new buyer's encryption watermark $c\varepsilon$, which is stored in the resale database during verification. Therefore, the new buyer's participation in the dispute resolution problem can be avoided.

5.7 Man-in-the-middle attack problem

In the proposed scheme, we are able to prevent an attacker from inserting or modifying any communication messages during the transaction. All data transferred between the buyer and the seller are encrypted or transmitted through a secure channel (such as the secure socket layer, SSL) to keep transaction data from being tampered with; thus, we can successfully curb the man-in-the-middle attack problem.

5.8 Anonymity problem

The solution to this problem is to keep the true identity of the new buyer concealed during the transaction. In the proposed protocol, we use an anonymous digital certification $Cert_N$ and a randomly generated one-time key pair $pk_B{}^i / sk_B{}^i$ to protect the new buyer's identity and to keep each transaction independent. The seller cannot discover the new buyer's true identity unless the new buyer is found to be guilty.

6. Comparisons

Next, we examine the requirements in the proposed scheme and compare our scheme with related researches. The comparisons are shown in **Table 1**, **Table 2** and **Table 3**.

Table 1. Security issues and dispute resolution comparison of related researches

Related researches / Issues	Cheung and Curreem [10]	Chen et al. [11]	Liu et al.[12]	Our Scheme
New buyer's right problem	Y	Y	Y	Y

Reseller's right problem	N	N	Y	Y
Unbinding problem	N	N	N	Y
Piracy tracing problem	Y	Y	Y	Y
Conspiracy problem	N	Y	Y	Y
Buyer's participation in the dispute resolution problem	N	Y	N	Y
Man-in-the-middle attack problem	N	N	Y	Y
Anonymity problem	N	Y	Y	Y
Proposed a dispute resolution method	Y	Y	N	Y

Compare with other buyer-reseller protocols, our scheme can solve security issues metioned in section 5. The proposed scheme also supports a complete dispute resolution method.

Table 2. Comparison of time complexity

	Schemes			
Phase	Cheung and Curreem [10]	Chen et al. [11]	Liu et al.[12]	Our scheme
Registration phase	NA	$T_{GKP}+ T_{CERT}+ 2T_E+ T_{SIG} +T_{AUC}$	NA	$T_{CERT}+ T_{SIG}+T_E$
Watermark generation phase	$2T_{CERT}+T_W$	NA	$T_{GKP}+T_W+ 2T_E +2T_{SIG}$	$T_D+T_{AUC}+T_{GKP}+ T_W+2T_E+ T_{SIG}$
Watermark insertion phase	$T_{CERT} + T_{EXT} + T_V+ T_X +T_\sigma+T_E+ T_{XOR}+T_D$	$T_{EXT} +2T_{AUC}+T_W+ T_\sigma+2T_E+T_{XOR}+T_D$	$2T_{AUC}+T_S+2T_E +2T_{XOR}+2T_D$	s(M) $(T_W+2 T_E+T_D)$
Copyright violator identification phase	$T_{EXT}+T_S$	NA	NA	$T_D + 2T_{AUC}$
Dispute resolution phase	$T_E+ T_{COMP}$	$T_{AUC}+ T_{SIG}$	NA	$2T_{\odot}+ 2T_{AUC}+ 4T_{COMP}$
Total	$3T_{CERT} +T_W +2T_{EXT} +T_V+ T_X + T_{COMP} +T_\sigma+2T_E+T_{XOR}+ T_D+T_S$	$T_{GKP}+T_{CERT}+2T_{SIG} +T_{EXT} + 4T_{AUC}+T_W+ T_\sigma+4T_E+T_{XOR}+T_D$	$T_{GKP}+T_W+ 2T_{SIG} + 2T_{AUC}+T_S+4T_E +2T_{XOR}+2T_D$	$T_{CERT}+ 2T_{SIG}+3T_E+ 2T_D+5T_{AUC}+T_{GKP}+ T_W+s(M)$ $(T_W+ 2T_E+T_D)+ 2T_{\odot}+ 4T_{COMP}$

Notes:

T_{CERT}：the time for generating a certificate

T_{EXT}：the time for extracting the transaction identifier V

T_W：the time for generating a watermark W

T_V：the time for generating the transaction identifier V

T_X：the time for generating a digital content X

T_σ：the time for generating a random permutation σ

T_E：the time for asymmetric encryption

T_D：the time for asymmetric decryption

T_{XOR}：the time for executing exclusive OR operation

T_{COMP}：the time for comparing operation
T_S： the time for searching the database
T_{GKP}： the time for generating a key pair
T_{SIG}： the time for generating a signature
T_{AUC}： the time for authentication
s(M): the blocks of the selected digital content for encryption of our protocol
$T_{\odot}$: the time for extracting algorithm

Since Liu et al.'s scheme [12] applies a double encryption method, zero knowledge verification techniques into their scheme, the computation requirements are large and it does not support a dispute resolution method. So, the proposed scheme is not practical. In addition, relative to other operations, the encryption, signature and decryption operations cost a lot during the transaction. Table 2 shows, the time complexity of our scheme approximates that of Chen et al.'s scheme [11] and is inferior to Cheung and Curreem [10]. However, Cheung and Curreem's scheme suffers from some security issues (as table 1 shows) and our scheme has less computation complexity in watermark insertion phase (it depends on the selected blocks $s(M)$). The original seller can determine the selected blocks by the importance of the digital content and the protected level. It differs from other related schemes (other schemes [10][11][12] require all the digital content to be encrypted or decrypted). So, the selected blocks are flexible and the proposed scheme can protect the key contents. Once the selected block $s(M)$ is large, the computation complexity approaches the related schemes [10][11]; otherwise, the proposed scheme also has good performance in computation complexity. Moreover, our scheme can provide a more secure protocol and dispute resolution method than others (as table 1 shows).

Table 3. Comparison of the communication cost

	Schemes			
Phase	Cheung and Curreem [10]	Chen et al. [11]	Liu et al.[12]	Our Scheme
Registration phase	NA	|Cert|+|PK|+|REQ|+ 2|E|+|SIG|+|PK|	NA	|ID|+2|Cert|+|SIG|
Watermark generation phase	2|Cert|+|W|	NA	|PK|+|REQ|+ 2|E|+ 4|SIG|	|E|
Watermark insertion phase	4|Cert|+2|V|+ 2|E|	4|E|+3|SIG|+2|PK|+ |Y|+|REQ|	3|E|	s(M)|E|
Copyright violator identification phase	Need not	Need not	Need not	Need not
Dispute resolution phase	|Cert|+|σ|+|Y|	|E|+|PK|+|W|+|SIG|	NA	|Y|+|M|+|PK|+|CW|+ |SIG|+|RI|+|σ|+⊙|
Total	7|Cert|+2|V|+ 2|E|+|W|+|σ|+ |Y|	|Cert|+4|PK|+2|REQ| +7|E|+5|SIG|+|PK|+ |Y|+|W|	|PK|+|REQ|+ 5|E|+ 4|SIG|	|ID|+2|Cert|+|SIG|+|E|+ s(M)|E|+|Y|+|M|+|PK|+ |CW|+|SIG|+|RI|+|σ|+|⊙|

Notes:
|Cert|: the length of the certificate

|W|: the length of the watermark
|V|: the length of the transaction identifier
|E|: the length of the encrypted digital content
|σ|: the length of the random permutation
|Y|: the length of the unauthorized digital content
|PK|: the length of the public key
|REQ|: the length of the request message
|SIG|: the length of the signature
|ID|: the length of the buyer's identity
|M|: the length of the digital content
|CW|: the length of the encrypted watermark
|RI|: the length of the resell information
|$\odot$|: the length of the watermark extracting algorithm
s(M): the blocks of the selected digital content for encryption of our protocol

As we know, the asymmetric cyrptography is not suitable to large-scale encryption or decryption. Compare with other buyer-reseller protocols, our scheme only selected the key content to encrypt and transmitted the encrypted digital content in step 3 of the watermark insertion phase. Under the consideration of the same implement encryption/decryption evaluation level, our scheme clearly incurs lower communication costs than related schemes. Therefore, our scheme is superior to the related schemes [10][11][12] in this respect..

The proposed protocol is able to satisfy all of the buyer-reseller protocol requirements. We protect all participators by combining the new buyer and the reseller's secret information based on private homomorphism and exponential calculus. We also make sure only the original seller can insert this secret into the digital content. Additionally, a fair arbitration mechanism is introduced to ensure that all parties benefit from our protocol.

7. Conclusions

In this paper, we protect the legal ownership of digital content and eliminate the TTP requirement by proposing a novel watermark generation mechanism to link the new buyer's watermark, the reseller's encryption watermark and the buyer's one-time key pair. Our scheme is able to overcome all known security problems involved in the buyer-seller watermark protocol, such as the buyer's right problem, the unbinding problem, the piracy tracing problem, the conspiracy problem, the buyer's participation in the dispute resolution problem, the man-in-the-middle attack problem and the anonymity problem. Further, the arbiter can verify the new buyer's watermark without having to decrypt it. Therefore, the proposed protocol becomes highly efficient and practical.

References

[1] N.D. Memon, P.W. Wong, "A Buyer-Seller Watermarking Protocol," *IEEE Transactions on Image Processing*," vol. 10, no. 4, pp. 643-649, 2001. Article (CrossRef Link)

[2] L. Qian, K. Nahrstedt, "Watermarking Schemes and Protocols for Protecting Rightful Ownerships and Customer's Rights," *Journal of Visual Communication and Image Representation*, vol. 9, no. 3, pp. 194-210, 1998. Article (CrossRef Link)

[3] C.L. Lei, P.L. Yu, P.L. Tsai, M.H. Chan, "An Efficient and Anonymous Buyer Seller Watermarking Protocol," *IEEE Transactions on Image Processing*, vol. 13, no. 12, pp. 1618-1626, 2004. Article (CrossRef Link)

[4] C.C. Chang, C.Y. Chung, "An Enhanced Buyer Seller Watermarking Protocol," in *Proc. of International Conference on Communication Technology*, vol. 2, pp. 1779-1783, Apr. 2003. Article (CrossRef Link)

[5] J. Zhang, W. Kou, K. Fan, "Secure Buyer-Seller Watermarking Protocol," *IEEE Proceedings*, vol. 153, pp. 15-18, 2006. Article (CrossRef Link)

[6] M. Kuribayashiv, H. Tanaka, "Fingerprinting Protocol for On-line Trade using Information Gap between Buyer and Merchant," *IEICE Transsactions. Fundamentals*, vol. E89–A, no.4, pp. 1108-1115, 2006. Article (CrossRef Link)

[7] C.I. Fan, M.T. Chen, W.Z. Sun, "Buyer Seller Watermarking Protocols with Off-line Trusted Parties,"*International Journal of Ad Hoc and* U*biquitous Computing*, vol. 4, no.1, pp. 36-43*,* 2009. Article (CrossRef Link)

[8] I.M. Ibrahim, S.H.N. El-Din, A.F.A. Hegazy, "An Effective and Secure Buyer Seller Watermarking Protocol," in *Proc. of third International Symposium on Information Assurance and Security (IAS 2007)*, pp. 21-26, 2007. Article (CrossRef Link)

[9] M. Deng, B. Preneel, "On Secure and Anonymous Buyer Seller Watermarking Protocol," in *Proc. of The Third International Conference on Internet and Web Applications and Services*, pp. 524-529, 2008. Article (CrossRef Link)

[10] S.C. Cheung, H. Curreem, "Rights Protection for Digital Contents Redistribution over the Internet," in P*roc. of the 26th Annual International Computer Software and Applications Conference (COMPSAC'02)*, Oxford, UK, pp. 105-110, 2002. Article (CrossRef Link)

[11] T. H. Chen, G.B. Horng, D.S. Tsai, "An Anonymous Buyer Reseller Watermarking Protocol," *Journal of the Chinese Institute of Engineers*, vol. 28, no. 3, pp. 535-538, 2005. Article (CrossRef Link)

[12] Q. Liu, Z. Chen, Z. Zhou, "Research on Secure Buyer Seller Watermarking Protocol," *Journal of Systems Engineering and Electronics,* vol. 19, no. 2, pp. 370-376, 2008. Article (CrossRef Link)

[13] R.L. Rivest, L. Adleman, M.L. Dertouzos, "On Data Banks and Privacy Homomorphisms," *Foundations of Secure Computation*, pp. 169-179, 1978. Article (CrossRef Link)

[14] P. Meerwald, A. Uhl, "A Survey of Wavelet-Domain Watermarking Algorithms," in *Proc. of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Content III*, San Jose, CA, vol. 4314, pp. 505-516, Jan. 2001. Article (CrossRef Link)

[15] I.J. Cox, J. Kilian, T. Leighton, T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, vol. 6, no.12, pp. 1673-1687, 1997. Article (CrossRef Link)

Chin-Ling Chen was born in Taiwan in 1961. He received the a B.S. degree in Computer Science and Engineering from the Feng Cha University in 1991; the a M.S. degree and Ph.D. in Applied Mathematics at National Chung Hsing University, Taichung, Taiwan, in 1999 and 2005 respectively. He is a member of the Chinese Association for Information Security. From 1979 to 2005, he was a senior engineer at the Chunghwa Telecom Co., Ltd. He is currently an associate professor of for the Department of Computer Science and Information Engineering at Chaoyang University of Technology, Taiwan. His research interests include cryptography, network security and electronic commerce.

Chin-Chang Chen was born in 1970. He received a B.S degree in the Department of Business Administration from National Central University, Taoyuan Taiwan in 1995. He received the a Masters degree in Computer Science from the Institute of Information Engineering and Computer Science, National Chung Hsing University (NCHU), Taichung, Taiwan, in 2009. His research interests include information security and cryptology.