A practical and secure buyer-seller watermarking protocol

Defa Hu*1, Qiaoliang Li2
1School of Information
Hunan University of Commerce
Changsha 410205, Hunan
China
hdf666@163.com
2School of Mathematics and Computer
Normal University
Changsha 410082, Hunan
China
qil@163.com

ABSTRACT: Digital watermarking is an emerging technology for combating copyright piracy. In real applications, the transaction between a buyer and a seller is done through a specific watermarking protocol, which enables the seller to successfully identify a traitor from a pirated copy, while preventing the dishonest seller from framing an innocent buyer. In this paper, we propose a new buyer-seller watermarking protocol. Compared to the previous works, it makes two improvements, which make it more practical. First, no third party is introduced and hence, the problem of the problem of the seller (or buyer) colludes with a third party to cheat the buyer (or seller) is solved. Second, double watermark insertion is avoided, and then the final quality of the watermarked content is higher and the result of the watermark detection is more accurate.

Categories and Subject Descriptors
C.2.2 [Network Protocols] Protocol architecture E.3 [Data Encryption]

General Terms: Digital watermarking, Watermarking protocols, Copyright piracy

Keywords: Digital watermarking, Digital copyright protection, Watermarking protocol, Copy deterrence

Received: 17 August 2010; Revised 13 October 2010, Accepted 19 October 2010

1. Introduction
The recent success of the Internet and the rapid development of information technology facilitate the proliferation e-commerce, where all types of digital data can easily be stored, traded, replicated, and distributed in digital form without a loss of quality. In the meantime, piracy becomes increasingly rampant as customers can easily duplicate and redistribute the received digital content to a large audience. To protect the digital copyright, ensuring the proper distribution and usage of digital content has become increasingly critical, especially considering the ease of manipulating digital data. Digital watermarking has developed as a prominent technology for protecting digital content from pirating, where a copyright notice is embedded into the distributed digital copies invisibly.

In a real application, each participant such as the buyer and the seller follows a secure buyer-seller watermarking protocol which combines digital watermarking and cryptography. A secure and fair buyer-seller watermarking protocol should enable a seller to successfully identify a traitor from a pirated copy, while preventing the seller from framing an innocent buyer. Buyer-seller watermarking protocol has been an active research topic in recent years and a number of buyer-seller watermarking protocols have been proposed [1,4,5,7,9]. Recent research indicates that a complete and sound buyer-seller watermarking protocol should be able to solve at least the following common problems.

– The piracy tracing problem: When a pirated copy is found somewhere, an honest seller should be able to trace pirated copies to the original buyer of the digital object effectively. Once the guilty buyer denies his responsibility for a copyright violation caused by him, the seller should be able to collect undeniable proof against the buyer. This problem usually is labeled as “seller’s security”.

– The anonymity problem: A buyer’s identity should be undisclosed until he is judged to be guilty. During the Internet transactions, one may expose her/his personal identity along with the information of the purchased product to others. As a result, how to protect the buyer’s privacy against the sellers is a quite important issue. If a seller can collect some sensitive data of a buyer, she/he may make use of the information to benefit from reselling these data to other parties or making criminal actions.

– The customer's rights problem: When a watermark is generated and inserted solely by the seller, a malicious seller may fabricate piracy to frame an innocent buyer, this could be a major concern for customers. For example, a malicious seller attempts to frame an innocent buyer by making and distributing a copy of the digital content which the buyer has purchased.

– The unbinding problem: The unbinding problem arises whenever a watermarking protocol fails to provide proper mechanisms on binding a chosen watermark to a given digital content or a specific transaction. Therefore, once the seller discovers a pirated copy in the market, he or she can transplant the watermark embedded in the pirated copy into another copy of a higher-priced digital content to produce made-up piracy so that he or she can be compensated further.

Although the existing watermarking protocols can solve the common problems mentioned above, there are two other drawbacks with them which make them impractical. First, a double watermark insertion appeared in all of these existing mechanisms on binding a chosen watermark to a given digital content or a specific transaction. Therefore, once the seller discovers a pirated copy in the market, he or she can transplant the watermark embedded in the pirated copy into another copy of a higher-priced digital content to produce made-up piracy so that he or she can be compensated further.

In a real application, each participant such as the buyer and the seller follows a secure buyer-seller watermarking protocol which combines digital watermarking and cryptography. A secure and fair buyer-seller watermarking protocol should enable a seller to successfully identify a traitor from a pirated copy, while preventing the seller from framing an innocent buyer. Buyer-seller watermarking protocol has been an active research topic in recent years and a number of buyer-seller watermarking protocols have been proposed [1,4,5,7,9]. Recent research indicates that a complete and sound buyer-seller watermarking protocol should be able to solve at least the following common problems.

– The piracy tracing problem: When a pirated copy is found somewhere, an honest seller should be able to trace pirated copies to the original buyer of the digital object effectively. Once the guilty buyer denies his responsibility for a copyright violation caused by him, the seller should be able to collect undeniable proof against the buyer. This problem usually is labeled as “seller’s security”.

– The anonymity problem: A buyer’s identity should be undisclosed until he is judged to be guilty. During the Internet transactions, one may expose her/his personal identity along with the information of the purchased product to others. As a result, how to protect the buyer’s privacy against the sellers is a quite important issue. If a seller can collect some sensitive data of a buyer, she/he may make use of the information to benefit from reselling these data to other parties or making criminal actions.

– The customer’s rights problem: When a watermark is generated and inserted solely by the seller, a malicious seller may fabricate piracy to frame an innocent buyer, this could be a major concern for customers. For example, a malicious seller attempts to frame an innocent buyer by making and distributing a copy of the digital content which the buyer has purchased.

– The unbinding problem: The unbinding problem arises whenever a watermarking protocol fails to provide proper mechanisms on binding a chosen watermark to a given digital content or a specific transaction. Therefore, once the seller discovers a pirated copy in the market, he or she can transplant the watermark embedded in the pirated copy into another copy of a higher-priced digital content to produce made-up piracy so that he or she can be compensated further.
In this paper, we propose a new buyer-seller watermarking protocol derived from an existing scheme presented in [1]. In our scheme, no third party is introduced, and then the conspiracy problem is avoided. In addition, the double watermark insertion problem is solved by embedding only one composite watermark, which is composed of two parts: one is generated secretly by the seller and the other by the buyer. Since none of them knows the exact composite watermark, thus, the buyer cannot remove the watermark from watermarked digital content, and the seller cannot frame an innocent buyer by fabricating piracy.

The remainder of this paper is organized as follows. In section 2, we overview some of the previous works which are associated with ours. In section 3, we introduce our watermarking protocol in detail. A concrete example of the proposed watermarking protocol is shown in Section 4. In Section 5, we analyze the security and practicality of the proposed scheme. A short conclusion is given in Section 6.

2. Related works

Qian and Nahrstedt [4] first proposed a watermarking protocol to solve the customer’s rights problem. In their protocol, the buyer sent the seller encrypted watermark which was embedded into the digital content by the seller. Since the buyer was the only one who knew the corresponding decryption key, he can prove his ownership to the digital content. However, this protocol has not solved the customer’s rights problem totally, as the seller can access the buyer’s watermarked copy and hence, a malicious seller can illegally redistribute an innocent buyer’s copy and accuses him of pirating while the innocent buyer can not prove his innocence.

In order to countermeasure this shortcoming along with solving the copy deterrence problem, Memon and Wong [7] proposed a buyer-seller watermarking protocol to deal with the customer’s right problem by preventing the seller from accessing the final watermarked copy. The center tool for achieving this scheme is an additive homomorphic public-key encryption scheme, which allows insertion of the encrypted watermarks directly into the encrypted content without prior decryption. An encryption scheme is said to be homomorphic if for any given public encryption key \( pk \), the encryption function \( E \) satisfies

\[
E_{pk}(x + y) = E_{pk}(x)E_{pk}(y),
\]

where \( x \) and \( y \) are the plaintexts. A general and more detailed introduction to homomorphic public-key cryptosystems can be found in [4]. There are several efficient homomorphic cryptosystems: ElGamal cryptosystem, Okamoto-Uchiyama cryptosystem, Pailler cryptosystem, RSA cryptosystem, Naccache-Stern cryptosystem, Benaloh cryptosystem and Goldwasser-Micali cryptosystem [6].

Although the scheme proposed by Memon and Wong can prevent the seller from accessing the final watermarked copy, it also introduced a new issue, the unbinding problem. In [1], the authors enhanced Memon and Wong’s scheme to solve the unbinding problem. In this protocol, the buyer and the seller set up a common agreement which called ARG that uniquely binds the digital object to the specified purchase transaction. In addition, this protocol uses the signature of watermark certification authority to bind the previously settled common agreement to the buyer’s watermark. This will prevent a malicious seller from embedding the buyer’s watermark into another higher-priced digital object provided that the two digital objects are sold to the same buyer. The anonymity problem is solved well by applying anonymous certificates, i.e., digital certificates without real identities of applicants to provide the buyer’s anonymity.

3. Proposed watermarking protocol

In our proposed scheme, we assume that the following assumptions hold. First, a public key infrastructure \( PKI \) is well deployed, such that each entity has a \( PKI \) certificate issued by the certification authority. Once this assumption holds, everyone is able to authenticate anyone else and the message exchange between any two parties can be made secure with no problem. Second, the watermarking scheme used should be robust so that nobody is able to remove the embedded watermark from the content without knowing the secret information. In addition, we also assume that a piece of digital content can be denoted by a vector.

The watermarking protocol that we present in this section has four sub-protocols: registration protocol, watermarking protocol, copyright violator identification protocol and dispute resolution protocol. There are four different roles are involved in our scheme: the seller (Alice), the buyer (Bob), the certification authority (CA) who is responsible for issuing anonymous certificates, and the arbiter (ARB) who adjudicates lawsuits against the infringement of copyright and intellectual property. We will use the following notation. We denote \( (pk_i, sk_i) \) as a public-private key pair, where \( i \) is the identity of its owner. \( Sign_i(M) \) denotes the signature of message \( M \) signed by \( i \) with his private key; \( Cert_i(I) \) denotes the digital certificate issued to party \( i \) by certification authority \( J \) and \( Enc_{pk}(M) \) denotes the ciphertext of message \( M \) encrypted with \( i \)’s public key, where \( E \) is the encryption function.

3.1 Registration protocol

If Bob wants to stay anonymous during the transaction, he may apply to \( CA \) for an anonymous certificate in advance, via the registration protocol presented in this subsection. An anonymous certificate is a normal digital certificate except that the content of its subject field is a pseudonym rather than the real identity of the applicant. By issuing the anonymous certificate to Bob, CA is responsible for binding this particular anonymous certificate to Bob. CA also guarantees that the binding is not revealed to any other party unless requested by the ARB when Bob is proven to be guilty. Alternatively, if anonymity is not necessary, Bob can skip the entire registration process and use his normal digital certification. To apply for an anonymous certificate, Bob first selects a key pair \( (pk_b, sk_b) \) and sends \( pk_b \) to CA. When CA receives the request from Bob, CA generates an anonymous certificate \( Cert_{CA}(pk_b) \) and sends \( Cert_{CA}(pk_b) \) to Bob. Liking as the previous work [1], we let the public key \( pk_b \) be the pseudonym associated with the anonymous certificate issued to Bob.

3.2 Watermarking protocol

To carry out a transaction, Bob and Alice follow the watermarking protocol described in this subsection (the basic interactive model is shown in Figure 1).

step 1. To acquire a copy of digital content \( \chi \), Bob first negotiates with Alice to set up a common agreement, ARG, which explicitly states the rights and obligations of both parties, and
specifies the digital content of interest. ARG uniquely binds this particular transaction to $X$ and can be regarded as a purchase order. In addition, the format of the watermark is also formulated in ARG. Note that Bob can use his pseudonym in the negotiation to keep his identity unexposed. Alternatively, since ARGs are different only in the part specifying the different digital content of interest, it is possible for Alice to generate ARGs beforehand and put them in a public place (e.g., her web site), along with the catalog of the digital contents to be sold, so that Bob may have anonymous access to ARGs.

**Step 2.** After the initial negotiation, Bob generates his watermark, $W_A$, which is a vector of real numbers with the length of $n$. $W_A$ is used to prevent Alice from framing him, which is generated according to the following method: the first $n_1$ elements are zeros and the last $n_2$ elements are chosen independently and randomly according to a fixed probability distribution which is provided in ARG. Here $n_1 + n_2 = n$. Then Bob encrypts $W_A$ using the encryption key $pk_A$ and the encryption function $E$ which has additive homomorphic property. Then he sends $pk_A$, $E$, $Cert_{CA}(pk_A)$, $E_{pk_A}(W_A)$, $Sign_{Bob}(E_{pk_B}(W))$, $ARG$, $W_A$, and $W_B$ to Alice.

**Step 3.** Upon receiving the request from Bob, Alice first verifies the validity of the certificate and signatures. If any of them is invalid, the transaction is aborted. Otherwise she generates the watermark $W_B$, which is a vector of real numbers with the length of $n$. $W_B$ is used to trace the source of the leakage by Alice, which is generated according to the following method: the first $n_1$ elements are chosen independently and randomly according to normal Gaussian distribution $N(0, 1)$ and the last $n_2$ elements are zeros. Here, $n_1 + n_2 = n$. After that, Alice generates the composite watermark $W$ and the watermarked copy according to the following method:

$$E_{pk_B}(W_B) = E_{pk_B}(W_A)_{E_{pk_B}(W_A)}$$

$$= E_{pk_B}(W_A + W_B)$$

$$E_{pk_B}(W_A) = E_{pk_B}(P)_{E_{pk_B}(W)}$$

$$= E_{pk_B}(P + W).$$

Here, the operator ‘+’ denotes the addition of vectors. Then Alice sends $E_{pk_B}(W_B)$ to Bob and stores $Cert_{CA}(pk_B)$, $Sign_{Bob}(E_{pk_B}(W_B))$, $E_{pk_B}(W_B)$, $ARG$, $W_A$, and $W_B$ as a new sales record with respect to the digital content $X$.

**Step 4.** Upon receiving $E_{pk_B}(W_B)$ from Alice, Bob decrypts it with his private key $sk_B$ and gets the watermarked copy $X_W$.

### 3.3 Copyright violator identification protocol

When a pirated copy $X'$ of a certain digital content $X$ owned by Alice is found in some where, the copyright violator identification protocol depicted in this subsection can be conducted to determine the identity of the responsible buyer with undeniable evidences. To trace the leak source of the pirated copy $X'$, Alice first extracts the first part of the composite watermark from $X'$ which is provided by her. Let $W'_B$ denote the watermark extracted corresponding to $W_B$. Using this extracted watermark $W'_B$, Alice then locates the buyer in her local transaction database to whom $Y$ was sold. The exact mechanism for finding a match completely depends on the watermarking scheme adopted. For robust watermarks this would generally be accomplished by correlating $W'_B$ with every watermark $W_i$ of the given digital content $X$ in transaction database and selecting the one with the highest correlation beyond a confidence threshold. Once a match is found, the buyer Bob is suspected to be a guilty buyer who redistributes the digital copy $X$.

### 3.4 Dispute resolution protocol

In case Bob denies that an unauthorized copy has originated from his version, Alice collects the associated information, $X'$, ARG, $W_A$, $E_{pk_B}(W_A)$ and $Cert_{CA}(pk_A)$, and sends them to ARB for arbitration. Once receiving the request from Alice, ARB asks $CA$ to decrypt $E_{pk_B}(W_A)$. $CA$ asks Bob to do this and sends $W_B$ to ARB. If Bob refuses to decrypt or he cannot do that correctly, it is clear to ARB that Bob may be the guilty buyer. Then, ARB generates the composite watermark $W = W_A + W_B$, and runs the corresponding watermark detection and extraction algorithm on $Y$ to extract the watermark denoted by $W'$. If the correlation between $W'$ and $W_B$ exceeds a confidence threshold, then Bob is considered as a guilty buyer. Otherwise, Bob is considered to be innocent.

### 4. An example of the proposed watermarking protocol

In this section, a concrete example of the proposed protocol is given, which uses a robust spread-spectrum watermarking technique proposed in [3] and a homomorphic public key cryptosystem proposed in [8]. Let $X = (x_1, x_2, \ldots, x_n)$ and $Y = (y_1, y_2, \ldots, y_n)$ be two vectors, for any given public encryption key, the used encryption function $E$ has the following property

$$E(X) \cdot E(Y) = E(x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

$$= E(X + Y).$$

Here, we assume that the digital content $X$ is a 2-dimension image whose size is $512 \times 512$. We also assume that the generated watermarks (vectors) $W_A$ and $W_B$ have a length of $n = n_1 + n_2 = 10000$ and both of them follow standard normal distribution denoted by $N(0,1)$. For simplicity, we let $n_1 = n_2 = 5000$.

To embed the encrypted composite watermark $E_{pk_B}(W)$ into $X$ without prior decryption, Alice first transforms $X$ into $DCT$ coefficients by performing $DCT$ transformation on $X$, and then the resulted coefficients are transformed into a descending sorted vector of length $L = 512 \times 512$. Let $x_1, x_2, \ldots, x_n$ be the $n$ largest coefficients and $y_1, y_2, \ldots, y_n$ be the rest of the coefficients. Then the composite watermark $W = (w_1, w_2, \ldots, w_n)$ is embedded into $x$ to yield the modified coefficients $x'$ according to the following method:


\[ E_{pk_A}(\chi') = E_{pk_A}(\chi)E_{pk_B}(W) \]
\[ = E_{pk_A}(\chi + W) \]
\[ = E_{pk_A}(x_1 + w_1, x_2 + w_2, \ldots, x_n + w_n). \]

Then \( \chi' \) is extended to a vector of length \( L \) by adding \( L - n \) zeros to the end of \( \chi' \) and \( \gamma \) is extended to a vector of length \( L \) by adding \( n \) zeros at the front of \( \gamma \). After that, \( \chi' \) and \( \gamma \) are assembled by

\[ E_{pk_B}(X_W) = E_{pk_A}(\chi')E_{pk_A}(\gamma) \]
\[ = E_{pk_A}(\chi' + \gamma). \]

When Bob receives \( E_{pk_B}(X_A) \) from Alice, he decrypts it with his private key and performs inverse DCT transformation on \( X_A \) to get the final watermarked copy. The original image and the watermarked image are shown in Figure 1. We can see that the watermarked image has no visible artifacts with PSNR (peak signal-to-noise ratio) of 48.6 db.

![Figure 2. (a) The original image. (b) The watermarked image with PSNR = 48.6 db. Note: the test image is from USC-SIPI image database whose URL is http://sipi.usc.edu/database/](image)

Once finding a pirated digital copy \( X' \) of \( X \), Alice extracts the watermark \( W \) according to the following method:

\[ W' = X' - X \]

Since the first 5000 elements of \( W \) are derived from the non-zero elements of \( W_s \) and the last 5000 elements of \( W' \) are derived from the non-zero elements of \( W'_s \). As a result, the first 5000 elements of \( W \) can represent \( W \) and the last 5000 elements can represent \( W'_s \). To decide whether \( W_s \) and \( W'_s \) match, Alice measure the similarity of \( W_s \) and

\[ Sim(W_A, W'_A) = \frac{W_A \cdot W'_A}{\sqrt{W_A \cdot W_A}}. \]

Here, the operator \( \cdot \) denotes dot product. The one who has the maximum similarity with \( W'_s \) is considered to be the source of the leakage. Similarity, during the dispute resolution phase, to decide whether \( W_s \) and \( W'_s \) match, the ARB only needs to compute \( Sim(W_s, W'_s) \) to determine the existence of \( W_s \) in \( X' \).

If \( Sim(W_s, W'_s) \) is larger than a threshold value, then a match is found to be first pointed out here that the security of the proposed watermarking protocol essentially depends on the security and robustness of the underlying watermarking scheme as well as the security of the cryptographic primitive.

For the customer’s rights problem. First, because Alice cannot access the watermarked content delivered to Bob, neither does she know Bob’s secret watermark \( W_s \). Therefore, Alice cannot accuse Bob by forging and distributing the replicas herself. On the other hand, Alice can’t forge Bob’s signature that explicitly binds \( E_{pk_B}(W_s) \) and \( pk_B \) to \( ARG \) which in turn binds to a particular transaction of the digital content \( X \). In this regard, it is infeasible for Alice to transplant Bob’s watermark to another content to fabricate piracy. Thus, the unbinding problems solved.

For the piracy tracing problem. First, once a pirated copy is found somewhere, Alice can locate the suspected buyer effectively. In addition, because only knows his watermark \( W_s \) but not the original content \( X \) and the composite watermark \( W \) which is generated from \( W_s \) and \( W'_s \). Therefore, under the assumption that the underlying watermarking scheme is robust, it is infeasible for Bob to remove his watermark \( W'_s \) from the watermarked content \( X_w \) neither can he claim that the copy was created by Alice. Because only Bob knows \( sk_B \) and \( W'_s \), no one can forge Bob’s copy.

For the anonymity problem. In our proposed scheme, the buyer’s privacy is well protected. Liking as the existing scheme [6], the proposed watermarking protocol takes advantage of anonymous certificates to preserve the anonymity of Bob during transactions. With the assistance of the CA, Bob can keep his real identity unexposed unless he is adjudicated to be guilty by ARB.

For the conspiracy problem. In our proposed scheme, the conspiracy problem is well solved. Since no third party is introduced into the digital content transaction in the proposed watermarking protocol, the problem of that Alice (or Bob) may collude with a third party to cheat Bob (or Alice) is avoided. In addition, the transaction is done between two parts, the buyer and the seller, which is similar to a real-world market and more practical.

For the double watermark insertion problem. Only one composite watermark \( W \) is inserted into the digital content \( X \), and then a double watermark insertion is avoided. As a result, the final watermarked copy has a higher quality, which is very important for some particular applications. In addition, the result of the tracing will be more accurate.

6. Conclusion

In this paper, we propose a new buyer-seller watermarking protocol which can solve all of the common problems, which are the customer’s rights problem, the unbinding problem, the anonymity problem and the piracy tracing problem. Furthermore, compared with those earlier works, we have made two important improvements. First, no third party is introduced, and then the conspiracy problem can be avoided. Since only two parties are involved and hence, the protocol is closer to reality and can be more easily implemented. Second, a double watermark insertion is avoided in our scheme, and then the quality of the final watermarked copy is higher and the result of the watermark detection is more accurate.

References


