Open access • Journal Article • DOI:10.1049/IP-IFS:20055069

Secure buyer-seller watermarking protocol — Source link

Jun Zhang, Weidong Kou, Kai Fan

Institutions: Xidian University

Published on: 03 Apr 2006

Topics: Trusted third party, Watermark, Secret sharing and Digital content

Secure buyer–seller watermarking protocol

J. Zhang, W. Kou and K. Fan

Abstract: In the existing watermarking protocols, a trusted third party (TTP) is introduced to guarantee that a protocol is fair to both the seller and buyer in a digital content transaction. However, the TTP decreases the security and affects the protocol implementation. To address this issue, in this article a secure buyer–seller watermarking protocol without the assistance of a TTP is proposed in which there are only two participants, a seller and a buyer. Based on the idea of sharing a secret, a watermark embedded in digital content to trace piracy is composed of two pieces of secret information, one produced by the seller and one by the buyer. Since neither knows the exact watermark, the buyer cannot remove the watermark from watermarked digital content, and at the same time the seller cannot fabricate piracy to frame an innocent buyer. In other words, the proposed protocol can trace piracy and protect the customer's rights. In addition, because no third party is introduced into the proposed protocol, the problem of a seller (or a buyer) colluding with a third party to cheat the buyer (or the seller), namely, the conspiracy problem, can be avoided.

1 Introduction

With the development of the Internet and e-commerce, it is clear that digital copyright protection has become an important issue. Digital watermarking has developed as a promising technology for protecting digital copyright. In the past, many digital watermarking algorithms have been proposed. The purpose of most of these algorithms is simply to achieve the goal of protecting digital copyright by embedding watermarks in digital content. This is not enough. A secure watermarking protocol is desirable [1–6] which uses the digital watermarking technique and a public key cryptosystem to protect the participants in a digital content transaction. Recent research indicates that a secure watermarking protocol should be able to resolve at least the following problems:

- The piracy tracing problem: when a pirated copy is found, an honest seller should be able to discover the pirate, who is an original buyer, and to collect undeniable proof against the buyer.
- The customer's rights problem: a malicious seller may fabricate piracy to frame an innocent buyer.
- The unbinding problem: a dishonest seller may transplant a watermark embedded in a pirated copy into a copy of higher-priced digital content to fabricate piracy.
- The anonymity problem: if required, the identity of a buyer should not be exposed unless he is proven to have committed piracy.
- The conspiracy problem: on the one hand, a malicious seller may collude with an untrustworthy third party to fabricate piracy to frame an innocent buyer; on the other hand, a malicious buyer may collude with an untrustworthy third party to confound the tracing of piracy by removing the watermark from digital content.

Qiao and Nahrstedt [1] first pointed out that the customer's rights problem exists in the watermarking protocols for tracing piracy. In [2], Memon and Wong propose a watermarking protocol to simultaneously resolve the piracy tracing problem and the customer's rights problem. In their scheme, watermark insertion is performed in the encrypted domain. The seller cannot access the watermarked digital content in its final form. Therefore, he cannot fabricate piracy to frame a buyer. In [3], Lei *et al*. address the unbinding problem. Their watermarking protocol binds a watermark to a common agreement (ARG) by the TTP's signature, and the ARG uniquely binds a particular transaction to a piece of digital content. Under their scheme, the seller cannot transplant the watermark embedded in a pirated copy into a copy of higher-priced digital content. In addition, the buyer can remain anonymous during the transaction through applying in advance to a certification authority (CA) for an anonymous certificate. In [4], Ju *et al*. propose an anonymous watermarking protocol in which a buyer can purchase digital content anonymously but the anonymity can be controlled.

Although a TTP can guarantee that a protocol is fair to both seller and buyer, the TTP decreases the security and affects the implementation of the protocol. If a third party introduced into a watermarking protocol is untrustworthy, the conspiracy problem has to be considered. Choi *et al*. [5] point out that in the existing watermarking protocols a malicious seller can collude with an untrustworthy third party to fabricate piracy to frame an innocent buyer [1–4]. Based on commutative cryptosystems, Choi *et al*. hope that a third party has no idea about the watermark the buyer chooses, and thus a seller cannot fabricate piracy even if he colludes with a third party. However, Goi *et al*. [6] find that this goal cannot be achieved through commutative cryptosystems. Furthermore, we find that the protocol in [5] does not take into account the collusion of a malicious buyer with an untrustworthy third party to remove the

IEE Proceedings online no. 20055069

doi:10.1049/ip-ifs: 20055069

Paper first received 21 September and in final revised form 3 December 2005

The authors are with the State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, 710071, P.R. China

E-mail: zhangj@mail.xidian.edu.cn

watermark from watermarked digital content. The conspiracy problem is still a bottleneck of the watermarking protocol.

In this article, a secure buyer–seller watermarking protocol derived from the one presented in [3] is proposed. In the protocol, no assistance of a third party is required, so that it avoids the conspiracy problem. Based on the idea of sharing a secret, a watermark embedded in digital content to trace piracy is composed of two pieces of secret information, one produced by the seller and one by the buyer. Since neither knows the exact watermark, the buyer cannot remove the watermark from watermarked digital content, and the seller cannot fabricate piracy to frame an innocent buyer.

The remainder of this article is organised as follows: in Section 2, a general description of our watermarking protocol is provided; an example of the proposed protocol is described in Section 3, and the security of the proposed protocol is analysed in Section 4. The article concludes in Section 5 with discussions of future avenues for research.

2 Secure buyer–seller watermarking protocol

In the proposed protocol, the interaction occurs only between a buyer and a seller, and there is no other party involved. Figure 1 shows a simplified trading model. Based on the protocol presented by Lei *et al*. in [3], the proposed protocol is similarly composed of three subprotocols: the registration protocol, the watermarking protocol and the identification and arbitration protocol.

2.1 Registration protocol

If a buyer B wants to remain anonymous during transactions, B randomly selects a key pair (pk_B, sk_B) and sends pk_B to a trusted CA [3]. When the CA receives pk_B, it generates an anonymous certificate, $\text{Cert}_{CA}(pk_B)$, and sends it back to B. Alternatively, if anonymity is not necessary, B may skip the entire registration process and use his normal digital certification.

2.2 Watermarking protocol

For a transaction, the buyer B and the seller S follow the watermarking protocol shown in Fig. 2, which consists of the following steps:

Step 1. B first negotiates with S to set up an agreement (ARG) which explicitly states the rights and obligations of both parties and specifies the digital content X. The ARG uniquely binds this particular transaction to X and can be regarded as a purchase order.

Step 2. B randomly selects a key pair (pk^*,sk^*) for this transaction and generates a secret SEC_B. Then, B signs the encrypted secret $E_{PK^*}(\text{SEC}_B)$ and ARG, $\text{Sign}_{sk^*}(E_{pk^*}(\text{SEC}_B),\text{ARG})$, and generates an anonymous certificate, $\text{Cert}_{pk_B}(pk^*)$. Finally, B transmits to S $\text{Cert}_{CA}(pk_B)$, $\text{Cert}_{pk_B}(pk^*)$, ARG, $E_{pk^*}(\text{SEC}_B)$, and $\text{Sign}_{sk^*}(E_{pk^*}(\text{SEC}_B),\text{ARG})$.

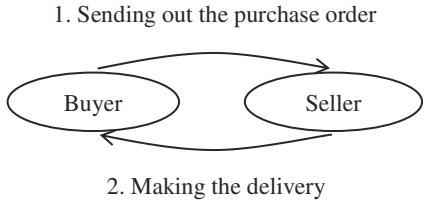

Fig. 1 *A simplified trading model*

Step 3. Upon receiving $\text{Cert}_{CA}(pk_B)$, $\text{Cert}_{pk_B}(pk^*)$, ARG, $E_{pk^*}(\text{SEC}_B)$ and $\text{Sign}_{sk^*}(E_{pk^*}(\text{SEC}_B),\text{ARG})$, S verifies the validity of the certificates and signature. If any of them is invalid, the transaction is aborted; otherwise, S generates a unique watermark V for this particular transaction and inserts it into X to get the watermarked digital content X', $X' = X \oplus V$. Then, S randomly generates a secret SEC_S. In the encrypted domain, S obtains the encrypted watermark $E_{pk^*}(W)$ as follows:

$$\begin{aligned} E_{pk^*}(W) &= E_{pk^*}(\text{SEC}_S) \otimes E_{pk^*}(\text{SEC}_B) \\ &= E_{pk^*}(\text{SEC}_S \oplus \text{SEC}_B) \end{aligned} \tag{1}$$

where $\oplus$ denotes addition and $\otimes$ denotes multiplication defined in the Galois field, respectively. S then inserts the second-round watermark through the following formula:

$$\begin{aligned} E_{pk^*}(X'') &= E_{pk^*}(X') \otimes E_{pk^*}(W) \\ &= E_{pk^*}(X' \oplus W) \end{aligned} \tag{2}$$

It is assumed that there exists a public key cryptosystem that is a privacy homomorphism with respect to addition, so that the encryption function E can be used in these equations. For example, the well-known Paillier public key cryptosystem [7] is a privacy homomorphism with respect to addition which can be used as a building block in different applications. A public key cryptosystem proposed by Bresson *et al*. [8] can also be applied to the above equations. Finally, S delivers $E_{pk^*}(X'')$ to B and stores V, $\text{Cert}_{CA}(pk_B)$, $\text{Cert}_{pk_B}(pk^*)$, ARG, $E_{pk^*}(\text{SEC}_B)$, $\text{Sign}_{sk^*}(E_{pk^*}(\text{SEC}_B),\text{ARG})$ and SEC_S as a new sales record with respect to the digital content X.

Step 4. After receiving $E_{pk^*}(X'')$, B decrypts it to obtain the correctly watermarked copy X'', $X'' = D_{sk^*}(E_{pk^*}(X''))$.

2.3 Identification and arbitration protocol

When a pirated copy Y of a certain digital content X is found, the identification and arbitration protocol is used to trace the pirate responsible and gather undeniable evidence.

S first extracts from Y the watermark V' inserted as the first watermark during the watermarking protocol. S then uses V' as a keyword to search his sales records with respect to X for a match. When a match is found, S collects the associated information, X' ($X' = X \oplus V_k$, where V_k is a keyword of the matched record), V, $\text{Cert}_{CA}(pk_B)$, $\text{Cert}_{pk_B}(pk^*)$, ARG, $E_{pk^*}(SEC_B)$, $\text{Sign}_{sk^*}(E_{pk^*}(\text{SEC}_B),\text{ARG})$ and SEC_S and sends them along with Y to an arbitrator (ARB).

Upon receiving X', V, $\text{Cert}_{CA}(pk_B)$, $\text{Cert}_{pk_B}(pk^*)$, ARG, $E_{pk^*}(\text{SEC}_B)$, $\text{Sign}_{sk^*}(E_{pk^*}(\text{SEC}_B),\text{ARG})$, SEC_S

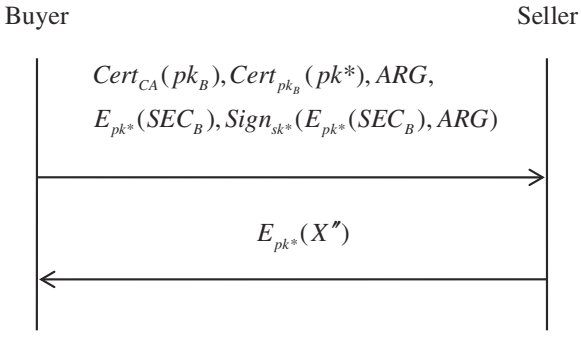

Fig. 2 *Details of the proposed watermarking protocol*

and Y, ARB verifies the validity of the certificates and the signature. If any of them is invalid, he rejects the case. Otherwise, ARB sends $\mathrm{Cert}_{\mathrm{CA}}(pk_{\mathrm{B}})$, $\mathrm{Cert}_{pk_{\mathrm{B}}}(pk^*)$ and $E_{pk^*}(\mathrm{SEC_B})$ to the CA and asks the CA to decrypt $E_{pk^*}(\mathrm{SEC_B})$. The CA orders B to do so, and sends $\mathrm{SEC_B}$ to ARB. In case B refuses to do the decryption, or cannot do so correctly, it is clear to ARB that B may be the pirate. Then, ARB computes $W = \mathrm{SEC_B} \oplus \mathrm{SEC_S}$, and runs the corresponding watermark detection and extraction algorithm (with X', W and Y as inputs) to determine the existence of W in Y. If W is indeed found in Y, ARB turns to the CA and asks for the real identity behind pk^*. Once the identity of the buyer who owns pk^* is revealed, ARB judges the buyer to be guilty and closes the case. If W is not detected in Y, the buyer is considered innocent, and his identity remains unexposed.

3 An example of the proposed protocol

In this Section, a specific example of the proposed protocol is provided which uses a robust spread-spectrum watermarking technique proposed by Cox *et al.* [9] along with the Paillier cryptosystem [7].

Cox *et al.* [9] embed a set of independent real numbers $\tilde{W} = \{w_1, w_2, \ldots, w_m\}$ drawn from $N(0,1)$ into the m largest DCT AC coefficients $\{x_1, x_2, \ldots, x_m\}$ of an image X using a suitable insertion formula to yield modified coefficients $\{x'_1, x'_2, \ldots, x'_m\}$. For example, the following insertion formula can be used:

$$x'_i = x_i + \alpha w_i \tag{3}$$

where α is a small constant. Through the inverse DCT, the watermarked image X' can be obtained.

The Paillier cryptosystem in [7] operates in Z_{n^2}, where n is the product of two very large primes p and q. A message x is encrypted as

$$y = E_g(x) = g^x r^n \bmod n^2 \tag{4}$$

where g is the public key and r is random number ($r < n$). The corresponding decryption function is

$$x = D_\lambda(y) = \frac{L(y^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n \tag{5}$$

where λ is the private key and function L is defined as $L(u) = (u-1)/n$.

In the proposed protocol, the watermark W embedded in a digital content is composed of the buyer's secret $\mathrm{SEC_B}$ and the seller's secret $\mathrm{SEC_S}$. It is assumed that $\mathrm{SEC_B}$ and $\mathrm{SEC_S}$ are each chosen through m independent random samples under the Gaussian distribution $N(0,1/2)$. Since the Paillier cryptosystem has the property that

$$E(x)E(y) = E(x+y) \tag{6}$$

$E_{pk^*}(W)$ can be derived as follows:

$$\begin{aligned} E_{pk^*}(W) &= E_{pk^*}(\mathrm{SEC_B})E_{pk^*}(\mathrm{SEC_S}) \\ &= E_{pk^*}(\mathrm{SEC_B} + \mathrm{SEC_S}) \end{aligned} \tag{7}$$

It is assumed that

$$\begin{aligned} \mathrm{SEC_B} &= \{\alpha\,\mathrm{sec}_{\mathrm{B}1}, \alpha\,\mathrm{sec}_{\mathrm{B}2}, \ldots, \alpha\,\mathrm{sec}_{\mathrm{B}m}\} \\ \mathrm{SEC_S} &= \{\alpha\,\mathrm{sec}_{\mathrm{S}1}, \alpha\,\mathrm{sec}_{\mathrm{S}2}, \ldots, \alpha\,\mathrm{sec}_{\mathrm{S}m}\} \\ W &= \alpha\tilde{W} = \{\alpha w_1, \alpha w_2, \ldots, \alpha w_m\} \end{aligned} \tag{8}$$

the arbitrary element w_i, ($w_i = \mathrm{sec}_{\mathrm{B}i} + \mathrm{sec}_{\mathrm{S}i}$, $i \in [1,\mathrm{m}]$) follows the Gaussian distribution $N(0,1)$. The seller first inserts the watermark V into the original image X to yield a watermarked image X'. He then inserts the watermark W into X' as follows:

$$\begin{aligned} E_{pk^*}(X'') &= E_{pk^*}(X')E_{pk^*}(W) \\ &= E_{pk^*}(X' + W) \end{aligned} \tag{9}$$

Note that each DCT coefficient of the digital content and each element of W are real numbers, which are represented with a fixed precision (e.g. 128 bits).

Finally, the seller sends the encrypted watermarked image $E_{pk^*}(X'')$ to the buyer. Upon receiving $E_{pk^*}(X'')$, the buyer obtains the uniquely watermarked copy of X by decrypting $E_{pk^*}(X'')$ using his private key sk^*.

4 Security analyses

In this Section, the security of the proposed watermarking protocol is analysed.

1. The secure buyer–seller watermarking protocol can resolve all the problems presented in Section 1:

- For the piracy tracing problem, because B knows only the secret $\mathrm{SEC_B}$ produced by himself and because B has no knowledge of the original digital content X and the watermark W, B is unable to remove the watermark W from a watermarked digital content X''. In addition, the proposed protocol provides mechanisms to unambiguously identify the guilty buyer once a pirated copy is found.
- For the customer's rights problem, because S knows only the secret $\mathrm{SEC_S}$ produced by himself and because he does not know the watermark W, S cannot fabricate piracy to frame B, as S has no access to the watermarked copy of the digital content in its final form.
- For the unbinding problem, because the signature $\mathrm{Sign}_{sk^*}(E_{pk^*}(\mathrm{SEC_B}),\mathrm{ARG})$ explicitly binds $\mathrm{SEC_B}$ to ARG, which uniquely specifies a particular digital content X, it is impossible for S to transplant the watermark into a copy of higher-priced digital content.
- For the anonymity problem, similar to the protocol of Lei *et al.* [3], the anonymity of the buyer can be retained during the transaction with the assistance of the CA unless the buyer is judged by ARB to be guilty of piracy.
- For the conspiracy problem, because no third party is introduced into a digital content transaction in the proposed protocol, the conspiracy problem is avoided.

2. In the proposed protocol, two watermarks V, and W, are inserted into a piece of digital content. When a pirated copy Y of a certain digital content X is found, S will extract V from Y and use it as a keyword to search his sales records with respect to X for a match. When a match is found, S can decide which original buyer produced the pirated copy and collect the associated information against the pirate. Then, W as undeniable evidence will be detected in Y by ARB to prove that the pirate is indeed the original buyer.

In order to simultaneously resolve the piracy tracing problem and the customer's rights problem, neither the seller nor the buyer should know the watermark W. Based on the idea of sharing a secret, the watermark W in the proposed protocol is composed of the buyer's secret and the seller's secret. The Paillier cryptosystem [7] has the property $E(W) = E(\mathrm{SEC_B})E(\mathrm{SEC_S}) = E(\mathrm{SEC_B} + \mathrm{SEC_S})$; that is, $W = \mathrm{SEC_B} + \mathrm{SEC_S}$. It is

clear from this equation that the possibility of the seller (or the buyer) guessing W is the same as the possibility of guessing SEC_B (or SEC_S). Therefore, it is almost impossible for the seller or the buyer to guess W.

The distortion of X'' can be controlled when two watermarks, V and W, are embedded. First, with knowledge of the original image X, S is able to choose a watermark V such that it will not affect the quality of X''. Second, generally speaking, each sample pair of SEC_B and SEC_S (a pair of small real numbers) is far smaller than DCT coefficients of digital content. Therefore, each element of W is smaller than DCT coefficients, which will not significantly affect the quality of X''. Furthermore, because without the knowledge of the watermark W, S knows the distribution of W and X, he can suggest a value of α to control the intensity of W, which can effectively decrease the distortion of X''.

3. In this article, based on the method proposed in [3], the anonymity of a buyer is retained. B applies to the CA for anonymous certification, $Cert_{CA}(pk_B)$, which can be used in multiple transactions. During a special transaction, B randomly selects a one-time key pair (pk^*,sk^*) and generates an anonymous certificate $Cert_{pk_B}(pk^*)$. Thus, B can use different key pairs for different transactions, which will significantly increase the security of a transaction.

For tracing piracy, the ARB requires the CA to decrypt $E_{pk^*}(SEC_B)$. The CA requires B to do it, and sends SEC_B to the ARB. Then the ARB can determine whether the watermark W is in the digital content Y. If W is indeed found in Y, the ARB rules that the buyer is guilty and closes the case. If W is not detected in Y, the buyer is considered innocent and his identity remains unexposed. The anonymity of the buyer can be controlled. It is clear from this article that there is no watermark CA. In other words, the proposed protocol is simpler than that in [3]. As the trade-off, the anonymity of the buyer is weaker than that provided in [3].

4. Compared with the existing watermarking protocols, the interaction in the proposed protocol occurs only between a buyer and a seller, which is closer to reality. In addition, the number of rounds of interaction and the amount of data transmitted in the proposed protocol are greatly reduced.

5 Conclusion

In this article, based on the protocol of Lei *et al.* [3] a secure buyer–seller watermarking protocol is proposed, without the assistance of a TTP, in which there are only two participants, a seller and a buyer. The proposed protocol can simultaneously resolve the piracy tracing problem, the customer's rights problem, the unbinding problem, the anonymity problem and the conspiracy problem. Since no third party is introduced, the proposed protocol is simpler and more secure than the existing watermarking protocol. However, there is a drawback in the proposed protocol; that is, the buyer's assistance is required to resolve the piracy dispute. We wish to improve this in the future research.

6 Acknowledgments

This work was supported by the Graduate Innovation Fund of Xidian University, NSFC grant 90304008 and CUDSFC 20040701001.

7 References

1 Qiao, L., and Nahrstedt, K.: 'Watermarking schemes and protocols for protecting rightful ownerships and customer's rights', *J. Vis. Commun. Image Represent.*, 1998, **9**, (3), pp. 194–210
2 Memon, N., and Wong, P.W.: 'A buyer–seller watermarking protocol', *IEEE Trans. Image Process.*, 2001, **10**, (4), pp. 643–649
3 Lei, C.-L., Yu, P.-L., Tsai, P.-L., and Chan, M.-H.: 'An efficient and anonymous buyer–seller watermarking protocol', *IEEE Trans. Image Process*, 2004, **13**, (12), pp. 1618–1626
4 Ju, H.S., Kim, H.J., Lee, D.H., and Lim, J.I.: 'An anonymous buyer–seller watermarking protocol with anonymity control', In Lee, P.J., and Lim, C.H. (Eds): Proc. ICISC 2002, *LNCS* **2587**, pp. 421–432
5 Choi, J.-G., Sakurai, K., and Park, J.-H.: 'Does it need trusted third party? Design of buyer–seller watermarking protocol without trusted third party', In Zhou, J., Yung, M., and Han, Y. (Eds): Proc. Applied Cryptography and Network Security 2003, *LNCS* **2846**, pp. 265–279
6 Goi, B.-M., Phan, R.C.-W., Yang, Y., Bao, F., Deng, R.H., and Siddiqi, M.U.: 'Cryptanalysis of two anonymous buyer–seller watermarking protocols and an improvement for true anonymity', In Jakobsson, M., Yung, M., and Zhou, J. (Eds): Proc. Applied Cryptography and Network Security 2004, *LNCS* **3089**, pp. 369–382
7 Paillier, P.: 'Public key cryptosystems based on composite degree residuosity classes', In Proc. Eurocrypt'99 1999, Stern, J. (Ed.): *LNCS* **1592**, pp. 223–238
8 Bresson, E., Catalano, D., and Pointcheval, D.: 'A simple public key cryptosystem with a double trapdoor decryption mechanism and its applications', In Laih, C.S. (Ed.): Proc. Aciacrypt, 2003, *LNCS* **2894**, pp. 37–54
9 Cox, I.J., Kilian, J., Leighton, T., and Shamoon, T.: 'Secure spread spectrum watermarking for multimedia', *IEEE Trans. Image Process.*, 1997, **6**, (12), pp. 1673–1687