2007

# Watermarking protocol of secure verification

Jun Zhang
*University of Wollongong*

Weidong Kou
*Xidian University*

Kai Fan
*Xidian University*

Lei Ye
*University of Wollongong*, lei@uow.edu.au

# Watermarking protocol of secure verification


## Abstract

The secure verification is important for watermarking protocols. A malicious arbitrator is able to remove an original watermark from an unauthorized copy of the digital content as a result of a security breach in the phase of arbitration and resell multiple copies of it with impunity. We propose a novel buyer-seller watermarking protocol of secure verification. In this scheme, a seller permutes an original watermark provided by a trusted Watermarking Certification Authority (WCA) and embeds it into digital content in an encrypted domain. In case an unauthorized copy is found, the seller can recover the original watermark from the watermark extracted from the copy and sends it to an arbitrator. Without the knowledge of permutations applied by the seller, the arbitrator is unable to remove the permuted watermark from the digital content. Hence, verification is secured. As an additional advantage of the proposed protocol, arbitration can be conducted without the need for the cooperation of the WCA or the buyer.



## Keywords

secure, verification, protocol, watermarking

## Disciplines

Engineering | Science and Technology Studies

## Publication Details

Zhang, J., Kou, W., Fan, K. & Ye, L. (2007). Watermarking protocol of secure verification. Journal of Electronic Imaging, 16 (4), 043002-1-043002-4.

Journal of Electronic Imaging 16(4), 043002 (Oct–Dec 2007)

# Watermarking protocol of secure verification

**Jun Zhang**
University of Wollongong
School of Information Technology and Computer Science
Wollongong, New South Wales 2522, Australia
E-mail: jz484@uow.edu.au

**Weidong Kou**
**Kai Fan**
Xidian University
The State Key Laboratory of Integrated Service Networks
Xi'an 710071, China

**Lei Ye**
University of Wollongong
School of Information Technology and Computer Science
Wollongong, New South Wales 2522, Australia

**Abstract.** *The secure verification is important for watermarking protocols. A malicious arbitrator is able to remove an original watermark from an unauthorized copy of the digital content as a result of a security breach in the phase of arbitration and resell multiple copies of it with impunity. We propose a novel buyer-seller watermarking protocol of secure verification. In this scheme, a seller permutes an original watermark provided by a trusted Watermarking Certification Authority (WCA) and embeds it into digital content in an encrypted domain. In case an unauthorized copy is found, the seller can recover the original watermark from the watermark extracted from the copy and sends it to an arbitrator. Without the knowledge of permutations applied by the seller, the arbitrator is unable to remove the permuted watermark from the digital content. Hence, verification is secured. As an additional advantage of the proposed protocol, arbitration can be conducted without the need for the cooperation of the WCA or the buyer.* © *2007 SPIE and IS&T.* [DOI: 10.1117/1.2804233]

## 1 Introduction

Digital copyright protection is an important issue in the development of e-commence. Digital watermarking is a promising technology for copy protection and copy deterrence. A number of digital watermarking algorithms have been proposed since the introduction of its concept. The essential idea behind the technology is to trace piracy by embedding watermarks in digital contents. To protect all parties' interests in a digital content transaction, a secure watermarking protocol is desirable in the process of establishing piracy. A secure watermarking protocol combines the digital watermarking techniques with cryptography.

Qiao and Nahrstedt[1] first pointed out that the customer's right problem exists in the watermarking protocols for tracing piracy. Memon and Wong[2] proposed a watermarking protocol to simultaneously resolve the piracy tracing problem and the customer's rights problem. Lei *et al.*[3] addressed the unbinding problem that exists in Memon and Wong's protocol. The secure verification problem is another important issue in the existing watermarking protocols. With the knowledge of a watermark provided by a seller as undeniable evidence to establish piracy, a malicious arbitrator (ARB) is able to remove the original watermark from an unauthorized copy and resell multiple copies of it with impunity. It was expected that asymmetric watermarking algorithms and watermark zero-knowledge proofs could resolve the problem.[4–7] However, existing asymmetric watermarking algorithms are not secure enough and watermark zero-knowledge proof systems are too complex for practical applications.

The work presented in this paper is derived from the research in Refs. 3 and 8. Lei *et al.*[3] proposed an efficient and anonymous buyer-seller watermarking protocol that successfully resolves the unbinding problem. In addition, during transactions the buyer can remain anonymous via the help of a trusted Certification Authority (CA) that is responsible to issue normal or anonymous digital certificates. However, this protocol has some drawbacks. First, the verification is insecure in the protocol. Second, it is not easy to simultaneously confine the distortion of the digital content caused by the watermark embedding and ensure the robustness of the two watermarks. Third, it is not convenient—and is therefore undesirable—that the cooperation of Watermarking Certification Authority (WCA) is required in the phase of arbitration. Kuribayashi and Tanaka[8] proposed a new watermarking scheme that embeds an information bit in the encrypted domain that ensures the plain value is not exposed. But the protocol that is based on additive homomorphic property has several issues. First, it cannot resolve the unbinding problem. Second, the verifi-

Paper 06175R received Oct. 3, 2006; revised manuscript received Mar. 28, 2007; accepted for publication May 1, 2007; published online Nov. 8, 2007.
1017-9909/2007/16(4)/043002/4/$25.00 © 2007 SPIE and IS&T.

cation is insecure in the protocol. Third, the use of zero-knowledge proofs significantly impedes the practicability of the protocol.

## 2 New Watermarking Protocol

The main idea of this paper is to resolve the secure verification problem and still retain the advantages of the protocols proposed in Refs. 3 and 8. The goals of the proposed new watermarking protocol are as follows:

1. A novel method is proposed to resolve the secure verification problem, which is much simpler and more secure than asymmetric watermark algorithms and watermark zero-knowledge proofs.
2. When an unauthorized copy is found, the seller and ARB can perform arbitration to establish piracy without the need for the cooperation of WCA or the buyer. This further enhances the practicability of the proposed protocol.
3. Only one watermark is embedded in a digital content and the distortion of a watermarked digital content can be effectively confined.

Similar to the protocol in Ref. 3, our proposed protocol is composed of three subprotocols: the registration protocol, the watermarking protocol, and the identification and arbitration protocol. These subprotocols are described as follows.

### 2.1 *Registration Protocol*

To remain anonymous in transactions, a buyer B randomly selects a key pair $(pk_B, sk_B)$ and sends $pk_B$ to CA.[3] When CA receives $pk_B$, it generates an anonymous certificate, $Cert_{CA}(pk_B)$, and sends it back to B. Then, as B's pseudonym, $pk_B$ will be used in a digital content transaction. It is assumed that CA uses the RSA cryptosystem,[9] such that the key pair $(pk_B, sk_B)$ is generated with the RSA algorithm.

If anonymity is not required, B may skip the entire registration process and use the normal digital certificate.

### 2.2 *Watermarking Protocol*

For protecting digital copyrights, B, a seller S, and the WCA implement the watermarking protocol, which consists of the following steps. The information is exchanged among B, S, and a trusted WCA in the proposed protocol. Figure 1 illustrates the flow of information among them and the details of a transaction in the protocol.

**Step 1.** For a transaction, B first negotiates with S to set up a common agreement ($ARG$), which explicitly states the rights and obligations of them, and specifies the digital content $X$. Note that $ARG$ uniquely binds this particular transaction to $X$ and contains S's commitment on the quality of $X$.

Then B randomly selects one public-private key pair $(pk^*, sk^*)$ according to additive homomorphic encryption algorithms, e.g., the Okamota–Uchiyama cryptosystem[10] and the Paillier cryptosystem,[11] for this transaction. After that, B signs $ARG$, $Sign_{pk_B}(ARG)$, and generates an anonymous certificate, $Cert_{pk_B}(pk^*)$. In this case, CA assures the legality of $pk_B$, and $pk_B$, in turn, assures the legality of $pk^*$.

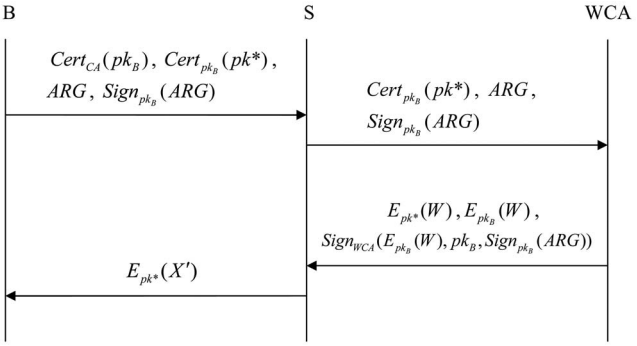


**Fig. 1** Information flow and details of a transaction in the proposed protocol.

Finally, B transmits $Cert_{CA}(pk_B)$, $Cert_{pk_B}(pk^*)$, $ARG$, and $Sign_{pk_B}(ARG)$ to S.

**Step 2**. Upon receiving $Cert_{CA}(pk_B)$, $Cert_{pk_B}(pk^*)$, $ARG$, and $Sign_{pk_B}(ARG)$, S verifies the validity of the certificates and signature. If any of them is invalid, the transaction is aborted; otherwise, $S$ sends $Cert_{pk_B}(pk^*)$, $ARG$, and $Sign_{pk_B}(ARG)$ to WCA and requests a valid watermark.

**Step 3**. When WCA receives $Cert_{pk_B}(pk^*)$, $ARG$, and $Sign_{pk_B}(ARG)$ from S, it verifies the validity of the certificate and the signature and aborts the transaction if either is invalid. Otherwise, it generates a watermark $W=\{w_1, w_2, w_3, \ldots, w_n\}$ specific to this transaction, where $w_i \in \{0,1\}$ $(i \in [1,n])$. Then WCA encrypts $W$ with $pk_B$ to get $E_{pk_B}(W)$ using the RSA encryption algorithm, and $W$ with $pk^*$ as $E_{pk^*}(W)=\{E_{pk^*}(w_1), E_{pk^*}(w_2), E_{pk^*}(w_3), \ldots, E_{pk^*}(w_n)\}$ using an additive homomorphic encryption algorithm, respectively. Finally, WCA computes $Sign_{WCA}(E_{pk_B}(W), pk_B, Sign_{pk_B}(ARG))$ and sends it, $E_{pk^*}(W)$, and $E_{pk_B}(W)$ back to S.

**Step 4**. Upon receiving the response, S randomly generates an reversible permutation function $\sigma$ of degree $n$ specific to the digital content $X$ to scramble the elements in $E_{pk^*}(W)$ to get $E_{pk^*}(W')=\sigma(E_{pk^*}(W))=E_{pk^*}(\sigma(W))=\{E_{pk^*}(w'_1), E_{pk^*}(w'_2), E_{pk^*}(w'_3), \ldots, E_{pk^*}(w'_n)\}$,[2] and performs the watermark insertion in the encrypted domain by computing $E_{pk^*}(X')=E_{pk^*}(X \oplus W')=E_{pk^*}(X) \oplus E_{pk^*}(W')$.[8] Afterwards, S sends $E_{pk^*}(X')$ to B and stores $Cert_{CA}(pk_B)$, $ARG$, $Sign_{pk_B}(ARG)$, $\sigma$, $E_{pk_B}(W)$, and $Sign_{WCA}(E_{pk_B}(W), pk_B, sign_{pk_B}(ARG))$ as a new sales record with respect to the digital content $X$.

**Step 5**. Upon receiving $E_{pk^*}(X')$, B decrypts it with his private key $sk^*$ by computing $X'=D_{sk^*}(E_{pk^*}(X'))$ and obtains the correctly watermarked copy $X'$.

### 2.3 *Identification and Arbitration Protocol*

When an unauthorized copy $Y$ of a certain digital content $X$ is found, the identification and arbitration protocol is used to trace and establish piracy with undeniable evidences.

S first extracts the watermark $\widetilde{W}$ from $Y$ and then searches the sales records with respect to $X$ for a match with the condition $E_{pk_B}(\sigma^{-1}(\widetilde{W}))=E_{pk_B}(W)$, where $\sigma^{-1}(\cdot)$ is the reverse permutation function. When a match is found, S

computes the original watermark $\tilde{W}'=\sigma^{-1}(\tilde{W})$. Then S collects the associated information, $Cert_{CA}(pk_B)$, $ARG$, $Sign_{pk_B}(ARG)$, $E_{pk_B}(W)$, and $Sign_{WCA}(E_{pk_B}(W),pk_B, sign_{pk_B}(ARG))$, and sends them with $\tilde{W}'$ to ARB. Upon receiving the information from S, ARB verifies the validity of the certificates, the signature, and $E_{pk_B}(\tilde{W}')=E_{pk_B}(W)$. If any of them is invalid, ARB rejects the case. Otherwise, ARB requests the real identity behind $pk_B$ from CA. Once the real identity of the buyer who owns $pk_B$ is revealed, ARB establishes the piracy against the revealed buyer.

## 3 Discussions

In this section, we examine how the design goals are achieved and analyze the security of the proposed watermarking protocol.

1. All the design goals set up in Section 2 are accomplished by the new watermarking protocol.

- The proposed protocol conveniently resolves the secure verification problem. The original watermark $W$ as undeniable evidence will be verified by ARB to establish the piracy against the original B, since S embeds the permuted watermark $W'=\sigma(W)$ into a digital content in the encrypted domain. Without S's permutation function $\sigma$, ARB has no knowledge of $W'$ and is unable to remove it from the unauthorized copy to resell multiple copies of it with impunity. Obviously, the method of watermark verification is simpler and securer than asymmetric watermarking algorithms and watermark zero-knowledge proofs.
- In the identification and arbitration phase, the cooperation of the WCA or B is not required. S extracts the watermark $\tilde{W}$ from the unauthorized copy and collects the associated information. Then the seller computes $\tilde{W}'=\sigma^{-1}(\tilde{W})$ using a reverse permutation function and sends it to ARB. ARB will verify $E_{pk_B}(\tilde{W}')=E_{pk_B}(W)$ and establish the piracy against B, who owns the public key $pk_B$.
- In the proposed protocol, only one watermark is embedded in a digital content. When an unauthorized copy of a digital content $X$ is found, S first extracts a watermark $\tilde{W}$ from it and then searches the sales records with respect to $X$ for a match with the condition $E_{pk_B}(\sigma^{-1}(\tilde{W}))=E_{pk_B}(W)$. When a match is found, S collects the associated information and sends it with $\tilde{W}'=\sigma^{-1}(\tilde{W})$ to ARB. The watermark $V$ for identifying the malicious B in the watermarking protocols given in Refs. 2 and 3 is not necessary in our proposed protocol. Furthermore, the distortion of the watermarked digital content caused by watermark embedding can be effectively confined using Kuribayashi and Tanaka's[8] watermark embedding method.

2. The proposed watermarking protocol can also address the following security issues.

- For the piracy tracing problem, because B has no knowledge of the original digital content $X$ and the permuted watermark $\sigma(W)$, B is unable to remove $\sigma(W)$ from a watermarked digital content $X'$. In addition, the proposed protocol provides a mechanism to unambiguously identify the malicious B once an unauthorized copy originated from B is found.
- For the customer's right problem, because S does not know the watermark $W$, S cannot produce a watermarked copy to frame B, since S gets no access to the watermarked copy of the digital content in its final form.
- For the unbinding problem, because the signature $Sign_{WCA}(E_{pk_B}(W),pk_B,sign_{pk_B}(ARG))$ explicitly binds $W$ to ARG, which uniquely specifies a particular digital content $X$, it is impossible for S to transplant the watermark into another copy of a higher-priced digital content.
- For the anonymity problem, similar to the protocol of Lei *et al.*,[3] the anonymity of B can be retained during the transaction with the assistance of CA unless ARB adjudges B to be guilty of piracy.

3. Considering the tradeoff between the robustness and the capacity, in the protocol by Kuribayashi and Tanaka[8] proposed, the watermark information has 32 bits. In our protocol, in order to prevent S from easily guessing the watermark $W$ according to $E_{pk_B}(W)$, the length of $W$ should be large enough, e.g., 512. We can improve both the robustness and the capacity of the watermark using the image-adaptive data hiding method given in Ref. 12. By the way, since the additive homomorphic encryption algorithms, such as the Okamota–Uchiyama cryptosystem[10] and the Paillier cryptosystem,[11] are random encryption algorithms, S is unable to guess the information bit according to $E_{pk^*}(w_i)$, $i\in[1,n]$.
4. B and S need to exchange information only once in our proposed protocol. B first sends a purchase order including $Cert_{CA}(pk_B)$, $Cert_{pk_B}(pk^*)$, $ARG$, and $Sign_{pk_B}(ARG)$ to S, and then S sends the encrypted watermarked digital content $E_{pk^*}(X')$ back to B. In a digital content transaction, B is not required to contact anyone else except S.[3] To get a digital content, B contacts S and provides the necessary information to S. Upon receiving the purchase order from B, S produces a watermarked digital content and delivers it to B, which completes the simple buyer-seller collaboration cycle.
5. Compared to Lei *et al.*'s protocol[3] and Kuribayashi and Tanaka's protocol,[8] the protocol proposed in this paper is securer and simpler. In addition, the amount of data transmitted is reduced and the practicability is improved. Our proposed protocol is well suitable for practical applications.

## 4 Conclusions

This paper proposed a watermarking protocol of secure verification based on PKI. A number of improvements are achieved over recent protocols in Section 3, which include the following:

1. A novel method is proposed to resolve the secure

verification problem, which is much simpler and securer than asymmetric watermarking algorithms and watermark zero-knowledge proofs.
2. ARB can determine whether the buyer produces the unauthorized copy according to the information provided by the seller without the need for the cooperation of the WCA or the buyer.
3. Only one watermark is embedded in a digital content, and the distortion of a watermarked digital content can be effectively confined.
4. The proposed protocol can also address the security problems in protocols discussed in Section 3. As a result, it is well suitable for practical applications.

Because the security of the watermarking protocols highly depends on the security and robustness of the underlying watermarking algorithms, our future work will include development of better watermarking algorithms that can operate in an encrypted domain.

## Acknowledgments

This work was supported by NSFC Grant 90304008, CUDSFC 20040701001 and Graduate Innovation Fund of Xidian University. Comments and suggestions from the reviewers were greatly appreciated and improved the quality of this paper.

## References

1. L. Qiao and K. Nahrstedt, "Watermarking schemes and protocols for protecting rightful ownerships and customer's rights," *J. Visual Commun. Image Represent* **9**(3), 194–210 (1998).
2. N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE Trans. Image Process.* **10**(4), 643–649 (2001).
3. C.-L. Lei, P.-L. Yu, P.-L. Tsai, and M.-H. Chan, "An efficient and anonymous buyer-seller watermarking protocol," *IEEE Trans. Image Process.* **13**(12), 1618–1626 (2004).
4. K. Gopalakrishnan, N. Memon, and P. L. Vora, "Protocols for watermark verification," *IEEE Multimedia* **8**(4), 66–70 (2001).
5. J. J. Eggers, J. K. Su, and B. Girod, "Public key watermarking by eigenvectors of linear transforms," in *Proc. Euro. Signal Process. Conf.*, Tampere, Finland (2000).
6. T. Furon and P. Duhamel, "An asymmetric watermarking method," *IEEE Trans. Signal Process.* **51**(4), 981–995 (2003).
7. A. Adelsbach, S. Katzenbeisser, and A.-R. Sadeghi, "Watermark detection with zero-knowledge disclosure," *ACM Multimedia Syst. J.* **9**(3), 266–278 (2003).
8. M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," *IEEE Trans. Image Process.* **14**(12), 2129–2139 (2005).
9. R. Rivest, A. Shamir, and L. Adelman, "A method for obtaining digital signatures and public key cryptosystem," *Commun. ACM* **21**(2), 120–126 (1978).
10. T. Okamoto and S. Uchiyama, "A new public-key cryptosystem as secure as factoring," in *Proc. Eurocrypt* 1403, 308–318 (1998).
11. P. Paillier, "Public key cryptosystems based on composite degree residuosity classes," in *Proc. Eurocrypt'99*, LNCS 1592, 223–238 (1999).
12. K. Solanki, N. Jacobsen, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Robust image-adaptive data hiding using erasure and error correction," *IEEE Trans. Image Process.* **13**(12), 1627–1639 (2004).

**Jun Zhang** received his BS and MS degrees both in communication engineering from Xidian University, P. R. China, in 2001 and 2004, respectively. He was a research student at the State Key Laboratory of Integrated Service Networks at Xidian University, P. R. China, from 2004 to 2006. He is currently pursuing his PhD degree in information technology and computer science at the University of Wollongong, Australia. His research interests include multimedia security and image retrieval.

**Weidong Kou** received his MS degree from Beijing University of Post and Telecommunications in 1982 his PhD degree from Xidian University, P. R. China, in 1985. He has published 7 books in English and over 100 papers in journals and conferences. He is an inventor with over 20 issued patents. He has worked at IBM, AT&T, and Siemens and has received various awards. He was associate director and principal researcher of the E-Business Technology Institute at the University of Hong Kong from 2000 to 2003. Before returning to IBM in 2004, he served as dean of the School of Computer Science and Engineering and the director of the State Key Laboratory of ISN at Xidian University. He was the Laureate of 2004 Friendship Award of China. Professor Weidong Kou is currently chief architect at the IBM Software Group in the Greater China Group. He is a senior member of IEEE. He has also served as associate editor for the *International Journal of Information Technology and Education*, a member of the editorial boards of the *International Journal of Electronic Commerce* and the *International Journal of Electronic Trade*, and guest editor for special issues on e-commerce for the *International Journal of Digital Libraries*. He was the general chair of 2004 IEEE International Conference on E-Commerce Technology for Dynamic E-Business.

**Kai Fan** received his BS and MS degrees from Xidian University, P. R. China, in 2002 and 2005, respectively, both in communication engineering. He is currently finishing his PhD degree in informatics system at Xidian University. He is working as a teaching assistant in the School of Telecommunications Engineering at Xidian University. His research interests include e-commence security and information security.

**Lei Ye** received his BEng and PhD degrees from Xidian University, China, in 1982 and 1989, respectively. He worked with the University of Electronic Science and Technology of China, Nanyang Polytechnic, Singapore, and the Australian Research Centre of Motorola. In 2004, he joined the University of Wollongong, Australia. His current research interests include image processing, retrieval and annotation, multimedia communication and computing, multimedia content management, rights management, and security. Dr. Ye is a senior member of the IEEE. He has served as session chair and member of technical committees of international conferences. He has also served as reviewer for *IEEE Transactions* and as assessor of the Australia Research Council Discovery Projects.