

A Secure and Efficient Buyer-Seller Watermarking Protocol

Yuping Hu

School of Information Science, Guangdong University of Business Studies, Guangzhou, 510320, P.R. China
 Hunan Institute of The Humanities, Science and Technology, Loudi, 417000, P.R. China
 Email: okhyp@yahoo.com.cn

Jun Zhang

School of Information Science, Guangdong University of Business Studies, Guangzhou, 510320, P.R. China
 Email: zhangjundan123@yahoo.com.cn

Abstract—The Digital watermarking technology has become increasing popular in the protection digital copyright. However, in the practical application, the watermarking algorithms should be combined with a secure copyright protection protocol to solve the copyright protection problems completely. In this paper, a novel buyer-seller watermarking protocol is proposed for piracy tracing, in which a memoryless Watermark Certification Authority (WCA) can offer a number of watermarks for a buyer simultaneously, avoiding itself being involved in each digital transaction operated between the buyer and the seller. Besides, in order to guarantee the anonymity of the buyer, the WCA can provide the buyer with an encrypted digital certificate and have it submitted directly to the seller by the buyer. In addition, the proposed protocol also can resolve other problems, such as the customer right problem, the binding attack problem, the anonymity problem, the conspiracy problem, the dispute problem. The analyses indicate that the proposed protocol is secure and practical.

Index Terms—copyright protection, digital watermarking, secure protocol

I. INTRODUCTION

With the development of the Internet and the E-Commerce, it is clear that digital copyright protection has become an important issue. Digital watermarking technology has developed as a promising technology for protecting digital copyright. The watermark is a signal that contains information about the copyright owner, which may be used for various applications, such as authentication, copyright and proof of ownership. However, in application, in order to solve the copyright protection problems completely, the watermarking algorithms should be combined with a secure copyright protection protocol^{[1][2][4][15]}.

Generally, there are three distinguished roles^{[3][13]}, such as a buyer, a seller and an arbiter (or Trusted Third Party, TTP) in a watermarking protocol for copyright protection.

Buyers are the end users of digital contents. Each copy of digital contents is uniquely watermarked to an identified buyer. Sellers are providers of the digital contents and own the rights of the contents, who employ their special watermarking techniques to embed watermarks into the digital contents offered to buyers. The arbiter is a TTP, who deals with watermark disputes between buyers and their sellers. Based on the evidence submitted by a content provider, the arbiter will decide whether a claim against a customer is justified or not. Recent research indicates that a secure watermarking protocol should be able to solve at least the following basic problems^{[4][5][6]}:

(1) 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.

(2) The customer's rights problem: A malicious seller attempts to frame an innocent buyer by making and distributing a copy of the product, which the buyer has purchased. And then, the seller may accuse the buyer of the illegal distribution.

(3) The binding problem: Upon discovering a pirated copy, the seller can fabricate piracy by transplanting the buyer's watermark into another digital content. Therefore, it is necessary to bind a chosen watermark with a specific transaction.

(4) The anonymity problem: If a seller can collect some sensitive data of a buyer, she/he may sell these data to other parties or commit crimes. So the identity of a buyer should not be exposed, unless he is proven to have committed piracy.

(5) 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.

(6) The dispute problem: A dishonest buyer may deny the purchasing record and benefit from illegal copies. Thus, disputes may happen between the buyer and the seller.

In this paper, we argue that a high efficient watermarking protocol should be able to resolve one more problem, that is,

(7) The on-line participation of a TTP: A TTP is required to participate in each transaction between a buyer and a seller. These interactions among the buyer, the seller and the on-line TTP may become a bottleneck of the entire protocol.

In this paper, we propose a novel buyer-seller watermarking protocol, which can solve all the problems mentioned above with an effective piracy tracing function. The rest of the paper is organized as follows: Section 2 describes the proposed watermarking protocol in detail. Section 3 analyses the security and efficiency of the proposed protocol. Section 4 summarizes our achievements.

II. RELATED WORK

In an attempt to tackle the customer's right problem, Qiao and Nahrstedt proposed an owner-customer watermarking protocol in Ref.[7]. In this protocol, the buyer (customer) first encrypts a predetermined sequence of bits with a secret key only known to him, and sends the encrypted data to the seller (owner).The seller then generates a unique watermark based on the encrypted data received and inserts it into a copy of the digital content, and sends the watermarked copy back to the buyer. Since only the buyer knows the secret key, he can prove to anyone his legitimate possession of the watermarked copy. However, when a pirated copy is found, the charge against the buyer pointed by the embedded watermark is objectionable because the seller in Qiao and Nahrstedt's protocol still has access to the watermarked copy in its final form. Consequently, the buyer's repudiation to the distribution of the pirated copy cannot be overruled in the trial.

In Ref.[8], Memon and Wong proposed a buyer-seller watermarking protocol to deal with the customer's right problem by preventing the seller from direct access to the final watermarked copy. We will go through the proposed protocol in this paragraph. There are two phases in their Buyer-Seller Watermarking Protocol, which are watermark generation phase and watermark insertion phase respectively. In this scheme, we assume that the seller is Alice, and the buyer is Bob. In order to generate the watermark, Bob has send a certification authority C and ask for a valid watermark. The watermark certification authority generates a random but valid watermark W and sends to Bob $E_{K_B}(W)$, which means the watermark is encrypted by Bob's public key. Besides that,the digital signature $Sign_c(E_{K_B}(W))$ is sent along with too. Here they assume that $E_{K_B}(W) = E_{K_B}(\{\omega_1, \omega_2, \dots, \omega_n\}) = \{E_{K_B}(\omega_1), E_{K_B}(\omega_2), \dots, E_{K_B}(\omega_n)\}$. That is, each of

the individual elements of the watermark W are encrypted as separate message but with the same key. As for the watermark insertion phase, there is a two party protocol between Alice and Bob that proceeds as follows:

(1) Bob sends to Alice the encrypted watermark, $E_{K_B}(W)$, along with the signature $Sign_c(E_{K_B}(W))$ of the certification authority C. Alice verifies $Sign_c(E_{K_B}(W))$ to make sure that $E_{K_B}(W)$ is indeed a valid watermark generated by C.

(2) Let X denote the image that Bob wishes to purchase from Alice .Alice generates a unique watermark for this transaction V , which she inserts into the image X to get the watermarked image X' . Note that in this step, Alice is free to use any watermarking scheme of her choosing, public or private, spatial domain or transform domain, liner or nonlinear. The purpose of the watermark V is to enable Alice to identify the specific user an illegal copy has potentially arisen from, that is, V is not the watermark that Alice will use to prove that Bob has made illegal copies of an image.

(3) Alice then generates a random permutation of the degree m , which she uses to permute the elements of the encrypted watermark $E_{K_B}(W)$ received from Bob. In other words, Alice computes $\sigma(E_{K_B}(W)) = E_{K_B}(\sigma(W))$. The above is true as $E_{K_B}(W)$ is of the form $\{E_{K_B}(\omega_1), E_{K_B}(\omega_2), \dots, E_{K_B}(\omega_n)\}$. and permuting first and encrypting later give the same result as encrypting later give the same result as encrypting first and permuting later.

(4) Alice inserts the permuted watermark into the already watermarked image X' . Since the watermark received from Bob is encrypted with Bob's public key, Alice inserts this second watermark in the encrypted domain also using the same key ,which is known to her. Inserting a watermark in the encrypted domain is possible as we assume that the public key cryptosystem being used is a privacy homomorphism with respect to \oplus , the operation that inserts a watermark in the image. In this step, Alice computes $E_{K_B}(X'') \oplus E_{K_B}(\sigma(W)) = E_{K_B}(X' \oplus \sigma(W))$. Alice transmits $E_{K_B}(X'')$ to Bob after that.

(5) Alice stores ID of Bob, $E_{K_B}(W)$, V , $Sign_c(E_{K_B}(W))$ and σ in Table_X, Table_X is a table of records maintained by Alice for image X containing one entry for each copy of X that she sells. The table contains the identity of the buyer ,the unique watermark V known to the particular buyer, the encrypted watermark $E_{K_B}(W)$ which she received from the buyer along with the certificate authority's signature $Sign_c(E_{K_B}(W))$ and the permutation σ .

(6) After computing the following equation, Bob will get the watermarked image X'' : $D_{K'_B}(E_{K_B}(X'')) = X'' = X' \oplus \sigma(W)$. Here, K'_B denotes the private key K_B , and $D()$ is the decryption function. We can see that Alice has no way to reproduce the watermark X since he has no idea what the private key of Bob is. On the other hand, Bob can't remove $\sigma(W)$ from X'' because he doesn't know the permutation function.

In spite of solving the customer's right problem, Memon and Wong's protocol has several issues. For example, the seller is able to intentionally transplant a watermark initially embedded in a copy of certain digital content into another copy of a completely different digital content, provided both copies are sold to the same buyer. We refer to this as the unbinding problem. In Ref.[9], Lei et al. address the unbinding problem. Their watermarking protocol binds a watermark to a common agreement (ARG) with the TTP's signature, and the ARG uniquely binds a particular transaction to a piece of digital content. In their scheme, the seller cannot transplant the watermark into a copy of higher-priced digital content. In addition, the buyer can remain anonymous during the transaction through applying to a certification authority (CA) for an anonymous certificate in advance. In Ref. [10] Ju H S et al. propose an anonymous watermarking protocol in which a buyer can purchase digital content anonymously but the anonymity can be controlled. In Ref.[11] J Choi et al. suggest a scheme to use the commutative cryptosystems which can solve the conspiracy problem of watermarking protocol in Ref.[10]. In Ref.[5], J. Zhang et al. propose a secure buyer-seller watermarking protocol, in which no assistance of a third party is required, so that it avoids the conspiracy problem. In Ref.[12], Chun-I Fan et al. propose a buyer-seller watermarking protocol with off-line trusted parties, in which a tamper-resistant WCA device is required to produce the necessary watermarks and signatures. However, the previous works proposed in Ref.[7] and Ref.[8] cannot solve the binding, the anonymity problem and the conspiracy problem. In the schemes of Ref.[8] and Ref.[11] on-line WCAs (Watermarking Certificate Authorities) are required, and the schemes of Ref.[9]-Ref.[10], Ref.[5] also need online CAs (Certificate Authorities) that must help a buyer to apply an anonymous certificate for every transaction. Therefore, these interactions among the buyer, the seller and the on-line CA may become a bottleneck of the entire protocol. Besides, In Ref.[11], WCA is required to maintain a database, and the scheme requires high computational complexity and communication, so it is not practical in implementation. In Ref.[12], for every seller, a tamper-resistant WCA device is required, thus the cost will be tremendous.

III. PROPOSED SCHEME

The proposed protocol employs the Public-Key Infrastructure (PKI) to attain several important achievements. In this section, we first define the roles and

notations to be used throughout the rest of this paper and explain the assumptions. Then, we continue to elaborate the three subprotocols that comprise the proposed protocol: the watermark generation protocol, the transaction protocol, and the identification and arbitration protocol.

In our scheme, there are four roles, i.e., a buyer (B), a seller (S), a Watermark Certification Authority (WCA) and an Arbiter (ARB). The buyer, the seller and the arbiter have been discussed in section 1. The WCA is responsible for the generation of random and valid watermarks, which can produce many watermarks for a buyer at a time and is not required to participate in each transaction between B and S. In order to guarantee the anonymity of the buyer, the WCA also can encrypt the certificate of the buyer and have it submitted to the seller by the buyer himself.

Some notations used in the proposed protocols are defined as follows:

(PK_I, SK_I) : A public-private key pair, where I is the identity of its owner. That is PK_I is I 's public key, while SK_I is I 's private key.

$Sign_{SK_I}(M)$: The signature of message M signed by I with his private key.

$E_{PK_I}(M)$: The ciphertext of message encrypted with I 's public key PK_I . The encryption can be performed by anyone.

$E_{SK_I}(C)$: The original message of cipher text C decrypted by I with SK_I .

$Cert_{CA}(I, PK_I)$: The digital certificate of the object I containing (PK_I, I) and the signature of the certificate authority (CA) on (PK_I, I)

\oplus : A watermark insertion operation.

σ : A random permutation of degree m function that is used to permute the elements of a vector.

An important assumption of the proposed watermarking protocol is that the encryption function used in PKI is privacy homomorphism with respect to the watermark insertion operation. By privacy homomorphism with respect to \oplus , we mean it has the property that $E_{PK_I}(a \oplus b) = E_{PK_I}(a) \oplus E_{PK_I}(b)$ holds for every a and b in the message space. For example, the well-known RSA cryptosystem is a privacy homomorphism [16] with respect to multiplication [17]. A public key encryption function that is a privacy homomorphism with respect to addition is given in Ref.[18].

Another assumption of the proposed watermarking protocol is that $\sigma(E_{PK_B}(W)) = E_{PK_B}(\sigma(W))$, the above is true when the watermarking scheme is linear, that $E_{PK_B}(W)$ is of the form

$\{ E_{PK_B}(\omega_1), E_{PK_B}(\omega_2) \dots E_{PK_B}(\omega_n) \}$ and permuting first and encrypting later gives the same result as encrypting first and permuting later^[8].

A. Watermarks Generation Protocol

To carry out a Watermarks Generation, B and WCA follow the watermarking generation protocol described in this subsection. Fig. 1 shows the interaction between B and WCA.

Step1: The buyer sends N (the required numbers of watermark) and his $Cert_{CA}(B, PK_B)$ to the WCA.

Step2: The WCA, after establishing the buyer's digital certificate, generates random but valid watermarks W_1, W_2, \dots, W_N and forms messages $M_{W_1}, M_{W_2}, \dots, M_{W_N}, M_B$ according to

$$M_{W_i} = \{ Sign_{SK_{WCA}}(PK_B || E_{PK_B}(W_i)), E_{PK_B}(W_i) \} \quad (1)$$

$$M_B = \{ Sign_{SK_{WCA}}(PK_B || E_{PK_{WCA}}(Cert_{CA}(B, PK_B))), PK_B, E_{PK_{WCA}}(Cert_{CA}(B, PK_B)) \} \quad (2)$$

Then, the WCA sends $\{ M_{W_1}, M_{W_2}, \dots, M_{W_N}, M_B \}$ to the buyer.

Step3: After receiving all the messages from the WCA, the buyer verifies the correctness of the signature in $\{ M_{W_1}, M_{W_2}, \dots, M_{W_N}, M_B \}$. If correct, the buyer stores $\{ M_{W_1}, M_{W_2}, \dots, M_{W_N}, M_B \}$ in his database.

B. Transaction Protocol

To carry out a transaction, B and S follows the transaction protocol described in this subsection. Fig. 2 shows the interaction between B and S.

Step1: The seller publishes the descriptions of all products she/he can provide. If the buyer decides to buy a product from the seller, B first negotiates with S to set up a common agreement ARG_X , which explicitly states the rights and obligations of both parties, and specifies the digital content of interest X . ARG_X uniquely binds this particular transaction to X and can be regarded as a purchase order.

Step2: The buyer selects a random M_{W_i} from his database and uses the included $E_{PK_B}(W_i)$ to form a purchase message

$$M_{ARG_X} = \{ Sign_{SK_B}(E_{PK_B}(W_i) || ARG_X), ARG_X \} \quad (3)$$

Then, the buyer sends $\{ M_{ARG_X}, M_{W_i}, M_B \}$ to the seller.

Step3: After receiving all the messages from the buyer, the seller verifies the correctness of the signatures in

$\{ M_{ARG_X}, M_{W_i}, M_B \}$. If correct, the seller generates a random permutation σ of degree m which he uses to permute the elements of the encrypted watermark $E_{PK_B}(W_i)$. In other word, the seller computes: $\sigma E_{PK_B}(W_i) = E_{PK_B}(\sigma W_i)$.

The seller prepares its watermark V and an encrypted watermarking version of the product X is produced by computing

$$\begin{aligned} E_{PK_B}(X') &= E_{PK_B}(X) \oplus E_{PK_B}(V) \oplus \sigma E_{PK_B}(W_i) \\ &= E_{PK_B}(X \oplus V \oplus \sigma(W_i)) \end{aligned} \quad (4)$$

Then, the seller transmits $E_{PK_B}(X')$ to the buyer.

Step4: The seller stores $\{ V, \sigma, \oplus, M_{ARG_X}, M_{W_i}, M_B \}$ in $Table_X$. $Table_X$ is a table of records maintained by the seller for content X containing one entry for each copy of X that she sells. The unique watermark V known only to her that corresponds to the particular buyer.

Step5: The buyer decrypts the data he receives from the seller to obtain a watermarked content X' . That is what the buyer computes:

$$X' = D_{SK_B}(E_{PK_B}(X')) = X \oplus V \oplus \sigma(W_i) \quad (5)$$

C. The identification and arbitration protocol

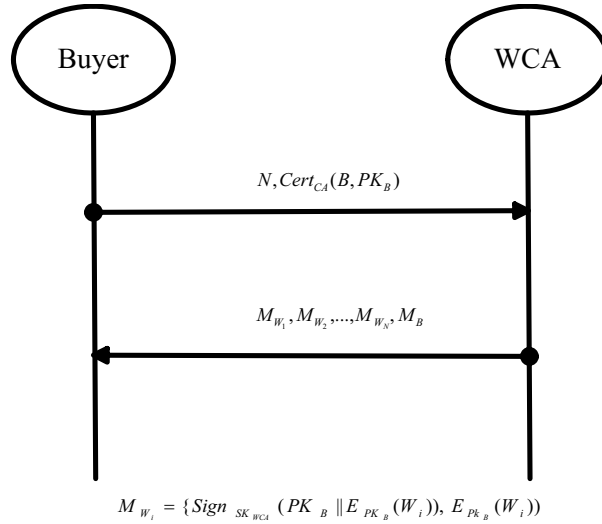
When a pirated copy Y of certain digital content owned by S is found in the market, the identification and arbitration protocol depicted in this subsection can be conducted to determine the identity of the responsible distributor, who was involved in some earlier transaction, with undeniable evidences. Fig. 3 shows the interaction among S , WCA and ARB.

First, the seller repeatedly takes every watermark in his database as the input of the watermark detection algorithm. If the detecting result is true for some input V , the seller can find the stored record $\{ V, \sigma, \oplus, M_{ARG_X}, M_{W_i}, M_B \}$ in $Table_X$ along with the illegal distribution Y to an arbitrator (ARB). The ARB checks if: (1) the content of Y is the same as the description in M_{ARG_X} ; (2) the signatures in M_{ARG_X}, M_{W_i}, M_B is correct.

If all of them are true, the ARB will ask the buyer to decrypt the $E_{PK_B}(W_i)$. Then, the buyer forwards W_i to the ARB securely. The ARB verifies W_i through encrypting it with the buyer's public key and comparing the encrypting result with $E_{PK_B}(W_i)$. The ARB inputs W_i, σ, V and Y to the watermark detection algorithm for detecting whether Y contains the watermark σW_i or not. If it is true, the ARB will ask the WCA to

decrypt $E_{PK_{WCA}}(Cert_{CA}(B || PK_B))$ and show the identity B of the buyer. The ARB will be convinced that B is the identity of the buyer since B can be linked to the

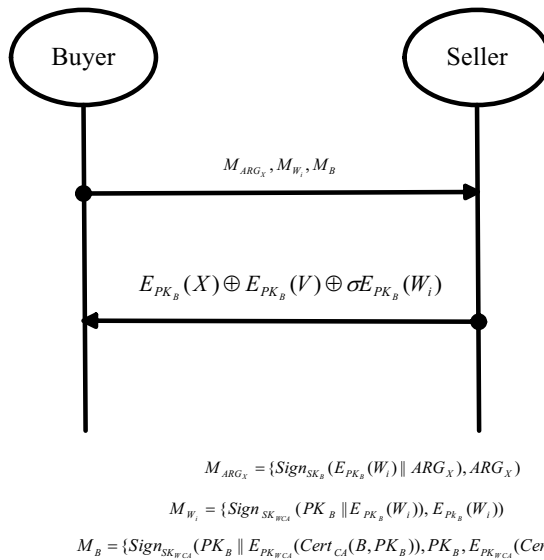
watermark W_i of the watermarked product Y through the above procedure



$$M_{W_i} = \{Sign_{SK_{WCA}}(PK_B || E_{PK_B}(W_i)), E_{PK_B}(W_i)\}$$

$$M_B = \{Sign_{SK_{WCA}}(PK_B || E_{PK_{WCA}}(Cert_{CA}(B, PK_B))), PK_B, E_{PK_{WCA}}(Cert_{CA}(B, PK_B))\}$$

Figure 1 . The Proposed Watermarks Generation Protocol.



$$M_{ARG_x} = \{Sign_{SK_B}(E_{PK_B}(W_i) || ARG_x), ARG_x\}$$

$$M_{W_i} = \{Sign_{SK_{WCA}}(PK_B || E_{PK_B}(W_i)), E_{PK_B}(W_i)\}$$

$$M_B = \{Sign_{SK_{WCA}}(PK_B || E_{PK_{WCA}}(Cert_{CA}(B, PK_B))), PK_B, E_{PK_{WCA}}(Cert_{CA}(B, PK_B))\}$$

Figure2. The proposed transaction protocol.

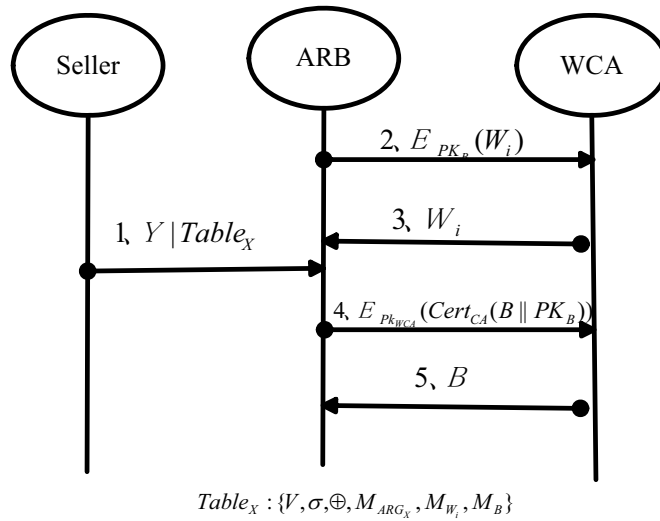


Figure3. The identification and arbitration protocol .

IV. SECURITY AND AVAILABILITY ANALYSES

The security of our scheme relies on the security of the underlying watermarking algorithm and cryptosystems. There are two major implementation differences between the proposed protocol and earlier works shown as follows: i) A memoryless Watermark Certification Authority (WCA) is introduced, that can produce many watermarks for a buyer at a time and is not required to participate in each

transaction of digital content between the buyer and its seller; ii) the WCA encrypts the certificate of a buyer and hands over the encrypted message to its seller via the buyer.

In this section, we will examine the security and efficiency of the proposed scheme and compare our scheme with those of Ref.[8], Ref.[9], Ref.[5], and Ref.[11]. The comparisons are summarized in Table I and Table II .

TABLE I. PROPERTY COMPARISONS

	[8]	[9]	[5]	[11]	[12]	Ours
The Piracy tracing problem	✓	✓	✓	✓	✓	✓
The customer right problem	✓	✓	✓	✓	✓	✓
The binding problem	×	✓	✓	✓	✓	✓
The anonymity problem	×	△	△	✓	✓	✓
The dispute problem	×	✓	✓	✓	✓	✓
The on-line participation of TTP(or TTP device)	×	×	×	×	×	✓

√ Solved ; △Partially; × Not solved

TABLEII .THE COMPUTATION COMPARISONS

	[8]	[9]	[5]	[11]	[12]	Ours
Encryption operations	2	3	3	2k+2	3	3
Decryption operations	1	1	1	4	1	1
⊕ operations	2	2	2	2	2	2
Signing operations	1	2	1	k	2	3

K: The number of watermarks

A. Security analysis

(1) Piracy tracing: Because B has no knowledge of the original digital content X and the permutation σ , he is unable to remove the watermark σW_i 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;

(2) Customer's rights protecting: Because S does not know the watermark W_i and can not access to the watermarked copy of the digital content in its final form, S cannot fabricate piracy to frame B;

(3) Free from the binding: Because the signature $Sign_{SK_B}(E_{PK_B}(W_i) || ARG_X)$ in M_{ARG_X} explicitly binds $E_{PK_B}(W_i)$ to ARG_X , which uniquely specifies a particular digital content X, it is impossible for S to transplant the watermark into a copy of any costly digital content;

(4) Complete anonymity on the part of the buyer: On the one hand, since $\{V, \sigma, \oplus, M_{ARG_X}, M_{W_i}, M_B\}$ has been recorded in the database, the seller cannot obtain any information about the identity of the buyer from it. Furthermore, the buyer's purchase request is sent through an anonymous channel, and the seller can only offer the encrypted product without knowing the buyer's identity in the protocol. Therefore, the privacy of the buyer is completely protected from being known to the seller during the transaction. On the other hand, the WCA has the buyer's identity, but it cannot recognize the digital content bought by the buyer. Thus the privacy of the buyer is also protected from the WCA.

(5) Free from the conspiracy: In our scheme, the WCA issues N watermarks and forms messages $M_{W_1}, M_{W_2}, \dots, M_{W_N}$, where the buyer selects a $E_{PK_B}(W_i)$ in a random M_{W_i} , so no one (except the buyer) knows the buyer's unique watermark. Furthermore, the conspiracy attack to our protocol cannot take effect.

(6) The dispute settlement: If a dishonest buyer attempts to deny his purchase of X' , the seller can reveal the stored record $\{V, \sigma, \oplus, M_{ARG_X}, M_{W_i}, M_B\}$ to the ARB. Then the ARB can find the identity of the buyer and the corresponding signature on ARG_X against the denying from the dishonest buyer.

B. Availability analyses

(1) The deploying of WCA: The cost of deploying trusted third parties (TTP) directly impacts the practicality of most security protocols. In reality, a memoryless TTP, which does not keep records of information associated with the requests received, is considered less expensive and is much more practical to implement. In our proposed watermarking protocol, WCA is not required to maintain a database of all watermarks generated because once generated, the

watermarks W_i ($i=1,2,\dots,N$) are used to form M_{W_i} and handed over to the buyer. When requested by ARB to disclose a specific watermark, WCA restores the watermark by decrypting the ciphertext provided by ARB. In addition, as for ARB, it simply reacts upon the requests from S and has nothing to remember.

(2) The participation of WCA in the transaction: WCA is an additional role between B and S. In the previous watermarking protocols, WCA is involved in each transaction, the availability of these protocols require the high reliability of WCA itself and the high stability of the communication network, and therefore those protocols are considered less practical. In order to reduce the overhead of an on-line WCA, in our proposed watermarking protocol, the WCA can produce many necessary watermarks for a buyer at a time. Since one watermark is required in each transaction between B and S, the times of interaction between B and WCA are reduced largely. Furthermore, the WCA is not required to participate in each transaction between B and S. Besides, in order to improve the reliability of WCA, cluster-based solutions can be used to construct a single node of WCA. On the other hand, deploying a distributed system with multiple nodes of WCA over the Internet solves the problem of network failures that may cause temporary or permanent disconnection from a particular node.

(3) The storage requirement for buyer and seller: In the proposed watermarking protocol, the burden of storing necessary information has been put on the buyer and the seller. It is reasonable because real-world buyers are very likely to have their individual information and real-world sellers are very likely to own sales records. The cost of keeping the necessary information can also be regarded as a part of an investment in the business. In addition, considering the ever-decreasing prices of various storage devices, the overhead introduced is actually negligible in running a business.

V. CONCLUSIONS

In this article, we have proposed a secure and efficient watermarking buyer-seller watermarking protocol, which can be free from all of the known attacks and problems, such as the customers' rights problem, the binding attack, the conspiracy problem, the dispute problem and can provide complete anonymity for the buyer as well. In addition, comparing with the earlier work, we also achieve two improvements as follows: 1) We address the importance of the off-line participation of a TTP. In order to solve the on-line participation of the TTP problem, a memoryless Watermark Certification Authority (WCA) is introduced, which can produce many watermarks for a buyer at a time and is not required to participate in each transaction of the digital content between the buyer and the seller. 2) We address the anonymity with control problems. In order to guarantee the anonymity with control, the WCA encrypts the certificate of a buyer and hands over the encrypted message to its seller via the buyer, so a buyer can purchase digital contents anonymously, but his anonymity can be revoked as soon as an

arbitrator adjudicates him to be guilty for any copyright violation.

ACKNOWLEDGMENTS

This work was supported by Scientific Research Fund of Hunan Provincial Education Department(06A031); Natural Scientific Research Fund of China (No. 60873198); Provincial Natural Science Foundation of Hunan ,China(06JJ0098) ; Natural Science Foundation of Department of Education of Guangdong Province (NO:05Z013) ; Guangdong Natural Science Foundation (NO:06023961).

REFERENCES:

- [1] Frattolillo, F, "Watermarking Protocol for Web Context. IEEE Transactions on Information Forensics and Security",vol.2, pp.50 – 363,Mar.2007.
- [2] Xiao-Su CHEN, Li-Gang LIU and Zheng-Din LU, "Design and Analysis of Digital Image Copyright Protection Security Protocol in Internet Environment", Chinese Journal of Computer, Vol. 2,pp.1722-1728, Sept. 2006.
- [3] Shing-chi Cheung, o-fung Leung and hangjie Wang, "A Commutative Encrypted Protocol for the Privacy Protection of Watermarks in Digital Contents", Proceedings of the 37th Hawaii International Conference on System Sciences, pp.94 - 103 ,Jan.2004.
- [4] QING Si-Han, "Twenty Years Development of Security Protocols Research", Journal of Software, Vol.14,pp. 1740-1752,Oct.2003.
- [5] Zhang, J , Kou, W and Fan, K, "Secure buyer-seller watermarking protocol".IEE Proceedings of Information Security, vol.153,pp.15 – 18,Mar.2006.
- [6] Katzenbeisser, S, "On the design of copyright protection protocols for multimedia distribution using symmetric and public-key watermarking ",12th International Workshop on Database and Expert Systems Applications,pp.815 – 819,2001
- [7] Qiao.L and Nahrstedt, "Watermarking schemes and protocols for protecting rightful ownership and customer's rights" ,Visual comm..and image representation,vol.23,pp. 194-210,Sept.1998.
- [8] Memon.N, and Wong.P.W, "A buyer-seller watermarking protocol", IEEE Transactions on Image Processing.vol. 4,pp.643-649,April 2001.
- [9] 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, vol.13, pp. 1618-1626, Dec.2004.
- [10] 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.
- [11] J. G. Choi, K. Sakurai, J. H Park, "Does it Need Trusted Third Party ? Design of Buyer-Seller Watermarking Protocol without Trusted Third Party" ,Proc. Applied Cryptography and Network Security'03, LNCS 2846, pp.265-279, 2003.
- [12] Fan, Chun-I, Chen, Ming-Te and Sun, Wei-Zhe , "Buyer-Seller Watermarking Protocols with Off-line Trusted Parties", MUE '07. International Conference on Multimedia and Ubiquitous Engineering, pp.1035 – 1040, April 2007.
- [13] S.Emmanuel and M.S.Kankanhalli, "A Digital Rights Management Scheme for Broadcast Video", CM/Spri-ng-er Multimedia Systems Journal, Vol. 8, No. 6,pp. 444 - 45 ,June ,2003.
- [14] Mina Deng, Bart Preneel, "On Secure and Anonymous Buyer-Seller Watermarking Protocol" ,Third International Conference on Internet and Web Applications and Services ,pp. 524-529, June 2008.
- [15] Tzung-Her Chen, Gwoboa Horng, "A lightweight and anonymous copyright-protection protocol", Computer Standards & Interfaces, Vol. 29(2),pp.229-237, 2007.
- [16] Rivest, A. Shamir, and L. Adelman, "A method for obtaining digital signatures and public key cryptosystems" , Commun. ACM, vol. 21, pp.120–126, 1978.
- [17] D. Stinson, Cryptography: Theory and Practice. Boca Raton, FL:CRC, 1995.
- [18] J. D. Cohen and M. J. Fischer, "Robust and verifiable cryptographically secure election scheme (extended abstract)", in Proc. IEEE 26th Annu.Symp. Foundations Computer Science, Portland, OR, pp. 372–382, Oct. 21–23, 1985.

Yuping Hu: Male, born in 1969, he received his B.S. degree in celestial survey from Chinese Academy of Science, China, in 1996 and his Ph.d. degree in computer science from Huazhong University of Science and Technology, Wuhan, China in 2005.He is currently pursuing the postdoctoral research in computer applications from Central South University, Changsha, China.

Dr.Hu is a professor in the College of Information, Guangdong University of Business Studies, Guangzhou, China. His current research interests include digital watermarking, image processing, multimedia and network security.

Jun Zhang was born in Sichuan, China in 1966. He received his Ph.D degree in computer science from Huazhong University of Science & Technology, China in 2003 and his M.Sc. degree in Mathematics from Lanzhou University in 1993. He had been a visiting postdoctoral Researcher in University College London, UK under Prof. Ingemar Cox's supervision. Now, he is the rector of Information Science School, Guangdong University of Business Studies. His research interest is information security such as data hiding, watermarking and privacy protection. In this field, He has published more than 30 papers. Moreover he had been in charge of some projects sponsored by National Natural Science Foundation of China and Guangdong Natural Science Foundation. He served as many workshop chairs, advisory committee or program committee member of various international IEEE.