Does It Need Trusted Third Party? Design of Buyer-Seller Watermarking Protocol without Trusted Third Party*

Jae-Gwi Choi[1], Kouichi Sakurai[2], and Ji-Hwan Park[1]

[1] Department of Information Security, Pukyong National Univ. 599-1 Daeyeon-dong Nam-ku Busan, Korea
jae@mail1.pknu.ac.kr, jpark@pknu.ac.kr

[2] Faculty of Information Science and Electrical Engineering, Kyushu Univ. 6-10-1 Hakozaki Higashi-ku Fukuoka, Japan
sakurai@csce.kyushu-u.ac.jp

Abstract. Buyer-seller watermarking protocol is a combination of traditional watermarking and fingerprinting techniques. For example, in applications where multimedia content is electronically distributed over a network, the content owner can embed a distinct watermark (a fingerprint), in each copy of the data that is distributed. If unauthorized copies of the data are found, then the origin of the copy can be determined by retrieving the unique watermark corresponding to each buyer. Recently, Ju and Kim proposed an anonymous buyer-seller watermarking protocol, where a buyer can purchase contents anonymously, but the anonymity can be controlled. They used two trusted parties: the watermark certification authority and the judge. The significance of this protocol is that it offered anonymity to watermarking protocol. But this protocol has the problem that honest buyers can be found as guilty, because sellers can recreate the same contents as the buyer's one if he/she colludes with the watermark certification authority and the judge. Thus this scheme must assume existence of the trusted third parties for its security. In this paper, we show shortcomings of this protocol and suggest a buyer-seller watermarking protocol that provides security of buyers and sellers without trusted third party.

1 Introduction

The current rapid development of new Information Technology and electronic commerce has resulted in a strong demand for reliable and secure copyright protection techniques for multimedia data. Over the past few decades, a considerable number of studies have been conducted on the design of methods that technically support the copyright protection of digital data. Copyright marking schemes have been proposed as the important class of these techniques. They are the embedding of marks into digital contents that can later be detected to identify owners (*watermarking*) or recipi-

* The first and third authors were partly supported by grant No.01-2002-000-00589-0 from the Basic Research Program of the Korea Science & Engineering Foundation and by University IT Research Center Project, MIC, Korea. It was done while the first author visits in Kyushu Univ. with the support of Association of International Education, Japan.

J. Zhou, M. Yung, Y. Han (Eds.): ACNS 2003, LNCS 2846, pp. 265–279, 2003.

ents (*fingerprinting*) of the content. While digital fingerprinting schemes enable a seller to identify the buyer of an illegally distributed content by providing each buyer with a slightly different version, digital watermarking schemes enable the seller/content owner to prove the rights of the contents by embedding the seller's information into the contents. Buyer-seller watermarking protocol is a combination of traditional watermarking and fingerprinting techniques.

1.1 Related Works

***Symmetric Schemes*:** Classical fingerprinting and watermarking schemes [QN98][Ne83] are symmetrical in the sense that the content owner knows the watermarks uniquely linked with the buyer. Thus, if another copy with this watermark turns up, the buyer can claim that the seller redistributed it. Because this could be done for example, by a malicious seller who may want to gain money by wrongly claiming that there are illegal copies around. Thus, one cannot really assign responsibility about redistribution to one of them.

***Asymmetric Schemes*:** This problem is overcome by asymmetric schemes [PS96][MW01]. Here, because only the buyer can obtain the exact watermarked (fingerprinted) copy, he/she cannot claim that an unauthorized copy may have originated from the seller. Hence, if an unauthorized copy is found, the seller can obtain a means to prove to a third party that the buyer redistributed it and he/she can identify a traitor/copyright violator. However the drawback of these solutions is that it did not provide a buyer's anonymity.

***Anonymous Schemes*:** To protect buyer's privacy two anonymous schemes have been suggested by Pfitzman et al [PW97] and Ju and Kim [JK02]. The idea is that the seller can know neither the watermarked content nor the buyer's real identity. Nevertheless the seller can identify the copyright violator later. This possibility of identification will only exist for a copyright violator, whereas honest buyers will remain anonymous.

Requirements of anonymous buyer-seller watermarking protocols can be listed as follows [JK02][PW97]:

1. **Anonymity:** A buyer should be able to purchase digital contents anonymously.
2. **Unlinkability:** Given two digital contents, nobody can decide whether or not these two contents were purchased by the same buyer.
3. **Traceability:** The buyer who has distributed digital contents illegally (traitor/copyright violator) can be traced.
4. **No Framing (Buyer's security):** An honest buyer should not be falsely accused by a malicious seller or other buyers.
5. **No Repudiation (Seller's security):** The buyer accused of reselling an unauthorized copy should not be able to claim that the copy was created by the seller or a security breach of the seller's system.
6. **Collusion Tolerance:** Attacker should not be able to find, generate, or delete the fingerprint by comparing the copies, even if they have access to a certain number of copies.

[PW97] scheme is inefficient and impractical because it is based on secure two-party computations [CD87] (It use general theorems like "every NP-language has a zero-knowledge proof systems" without presenting explicit protocols) with high complexity. Later, [PS00] suggested an efficient method without secure two party computations. But this method is also impractical because it used [BS95] scheme as a building block for collusion resistance. In [BS95], their code needed for embedding is so long that the overall system cannot be practical. Recently, [JK02] proposed an anonymous buyer-seller watermarking protocol, adding anonymity and unlinkability to [MW01] scheme. [JK02] scheme and [MW01] scheme used Cox's invisible watermarking algorithm [CK97] as a building block. [JK02] scheme is a significant model in the sense that it offered the anonymity of a buyer to watermarking protocol. But the problem of this protocol is that it cannot provide security of sellers and buyers, because a seller can recreate the buyer's copy if he/she colludes with the watermark certification authority and the judge.

1.2 Our Contributions

In this paper, we suggest secure buyer-seller watermarking protocol against conspiracy attack, which can solve the problem of [JK02] scheme. '*Conspiracy attack*' is means that a seller colludes with the watermark certification authority or the judge in order to recreate buyer's copy for his/her gain.

We compare the features of our proposal with [JK02], [MW01] in Table 1.

Table 1. Comparison of our proposal with [MW01] and [JK02]

Features	[MW01]	[JK02]	Our Proposal
Anonymity	No Offer	Offer	Offer
Unlinkability	No Offer	Offer	Offer
No two-party computation	Yes	Yes	Yes
No Framing	No Offer[1]	No Offer[2]	Offer
No Repudiation	No Offer[1]	No Offer[2]	Offer
Participators of Identification protocol	Arbiter, seller, Buyer	Judge, watermark certification authority, seller	Arbiter, watermark certification authority, seller, buyer

1: [MW01] scheme provides the pertinent function only if the watermark certification authority is memoryless and not malicious.

2: [JK02] scheme provides the pertinent function only if the watermark certification authority and the judge are not malicious.

The most meaningful feature of our scheme is that there is no need to assume the trusted third party (the watermark certification authority and the judge)'s honesty. On the contrary, [JK02] and [MW01] must assume that the watermark certification

authority does not collude with a seller or a buyer for security of their protocols, because the watermark certification authority knows the buyer's unique watermark. Besides, [JK02] scheme also must assume honesty of the judge, because a buyer's secret key is encrypted with the judge's public key. Since, the buyer's secret key is used in encryption of content and anonymity offering in [JK02] scheme, it must not be revealed. And, the judge of [JK02] scheme is not an arbitrator but the fixed party from the first stage (watermark generation protocol). On the other hand, the judge of our scheme and [MW01] scheme is a complete arbitrator because the judge is not involved in other protocols except identification protocol.

1.3 Our Approach

The main idea of our scheme is to use a commutative cryptosystems in watermark generation protocol in order to prevent conspiracy attack. In our scheme, the watermark certification authority issues the buyer's unique watermark to the buyer but he cannot know which watermark the buyer chose. Thus even if a seller colludes with the watermark certification authority, he cannot recreate the buyer's copy. The second idea is that buyers generate two secret keys by splitting the original secret key corresponding with her real identity. One is used in encryption of content and the other is used in her owns anonymity. In our scheme, the others except the buyer cannot know the buyer's secret key will be used in decryption. Thus the others cannot recreate the same watermarked contents as the buyer's one, if computing discrete logarithms is hard.

The rest of this paper is organized as follows. First, [JK02] scheme is described briefly and its shortcomings are discussed in Section 2. Next, cryptographic primitive is described in Section 3. Then, the proposed buyer-seller watermarking protocol is described in detail in Section 4 and various features of the proposed scheme are analyzed in Section 5. Finally, we conclude in Section 6.

2 Overview of the Attacked Scheme

In this section we briefly review the construction proposed in [JK02]. For simplicity we use the same notations.

2.1 Ju and Kim's Scheme

Preprocessing: All participants have a pair of a private key and a public key (sk, pk) certificated by certificate authority (CA).

Watermark Generation: A buyer generates an anonymous key pair of a private key and a public key (sk_B^*, pk_B^*). A buyer generates $C = E_{pk_j}(sk_B^*)$ and *cert* proving

that sk_B^* is a discrete logarithm or e-th root of a given pk_B^* without disclosing sk_B^* using a verifiable encryption scheme[1] (E). In here, pk_J is the public key of the judge. After the buyer transmits C, pk_B^*, signature of $pk_B^* : sign_{sk_B}(pk_B^*)$ and the certificate $cert$ to the watermark certification authority, the authority verifies the certificate. If it is verified, the watermark certification authority is convinced that C is indeed the encryption of sk_B^*. Then, the watermark certification authority generates a watermark $W = \{w_1, w_2, \cdots, w_n\}$ randomly and sends to the buyer the anonymous public key pk_B^* and the watermark encrypted with the buyer's anonymous public key $w = E_{pk_B^*}(W)$ along with $s = sign_{sk_w}(w \| pk_B^*)$, which certifies the validity of the watermark and also ensures that pk_B^* was used to encrypt W as public key. The watermark certification authority stores $B, w, s, pk_B^*, sign_{sk_B}(pk_B^*)$, and $(C, cert)$ in $Table_W$. Here $\|$ denotes a concatenation and the encryption algorithm is homomorphic[2].

Watermark Insertion: A buyer sends $pk_B^*, E_{pk_B^*}(W), s$ to the seller to obtain a watermarked content. By verifying the signature with the watermark certification authority's public key, the seller is convinced of the watermark's validity. If the verification holds, the seller generates a unique watermark V and embeds it into multimedia content X. Let X' be the watermarked content with V. To embed the second watermark W generated by the watermark certification authority into X' without decrypting $E_{pk_B^*}(W)$, the seller encrypts the watermarked content X' with pk_B^* and finds the permutation σ satisfying $\sigma(E_{pk_B^*}(W)) = E_{pk_B^*}(\sigma(W))$. Because of the homomorphic property of the encryption algorithm E used by the watermark certification authority, the seller can compute watermarked content $E_{pk_B^*}(X'')$. Where $\oplus$ denotes the embedding operation. The seller transmits the computed $E_{pk_B^*}(X'')$ to the buyer and stores pk_B^*, w, s, σ and V in his/her table $Table_B$.

$$E_{pk_B^*}(X'') = E_{pk_B^*}(X') \oplus \sigma(E_{pk_B^*}(W)) = E_{pk_B^*}(X \oplus V) \oplus E_{pk_B^*}(\sigma(W))$$
$$= E_{pk_B^*}(X \oplus V \oplus \sigma(W))$$

---

[1] The idea is that if A and B wish to exchange their signatures on some message, they will first exchange verifiable encryption of them, using as E the public key of some trusted third party. If this was successful, it will be safe for A to just reveal his signature to B. Even if B never answers, A can get B's signature by having the trusted party decrypt it [CD98].

[2] A public key encryption functions $E : G \to R$ defined on a group $(G, \cdot)$ is said to be homomorphic if E forms a homomorphism. That is, given $E(x)$ and $E(y)$ for some unknown $x, y \in G$, anyone can compute $E(x \cdot y)$ without any need for the secret key. In other words, by privacy homomorphism with respect to $\oplus$, it means it has the property that $E_{pk}(x \oplus y) = E_{pk}(x) \oplus E_{pk}(y)$.

Copyright Violator Identification: When an illegal copy Y of an original content X is discovered, the seller extracts the unique watermark U in Y using detection algorithm. Then, he/she finds the buyer's information $pk_B^*, E_{pk_B^*}(W), s, \sigma$ stored with V with the highest correlation by examining the correlations of extracted watermark U and all $V's$ in the $Table_B$. And the seller sends them with X, Y to the judge. The judge verifies $sign_{sk_B}(pk_B^*)$ and $cert$ with the help of the watermark certification authority, and recovers the buyer's anonymous private key sk_B^*. If the verification success, judge computes $\sigma(W)$ and checks the existence of $\sigma(W)$ in Y by extracting the watermark from Y and estimating its correlations with $\sigma(W)$. If there exists $\sigma(W)$, the buyer is guilty and the buyer's ID (B) is revealed to the seller.

2.2 Analysis of the Scheme

2.2.1 Observations on Security

This scheme is very efficient in the sense that identification protocol is carried out without any help of the accused buyer. But the most undesirable issue of [JK02] is that the seller can recreate the buyer's copy if he colludes with the watermark certification authority and the judge. Thus the seller can cheat an honest buyer in this scheme.

- **Conspiracy Attack I: Collusion of the Seller, the Watermark Certification Authority and the Judge**

  To forge illegal copy, Y with the special watermark W, first the seller sends pk_B^*, s received from a buyer to the watermark certification authority. The watermark certification authority searches for the buyer's information, $[w = E_{pk_B^*}(W), C = E_{pk_J}(sk_B^*), pk_B^*]$, corresponding with pk_B^*, s in $Table_W$ and sends it (C) to the judge. The judge decrypts C and sends sk_B^* to watermark certification authority. The watermark certification authority decrypt w using sk_B^* received from the judge and sends it to the seller. Then, the seller can recreate the buyer's copy because he/she knows the buyer's unique watermark, W.

- **Conspiracy Attack II: Collusion of the Seller and the Judge**

  [JK02] insists that only the buyer can decrypt the watermarked contents, because the watermarked content $E_{pk_B^*}(X'')$ encrypted with the buyer's anonymous public key pk_B^*. However in this protocol, a seller can obtain $C = E_{pk_J}(sk_B^*), pk_B^*$ are transmitted through insecure channel in the watermark generation protocol. If a seller obtains C, pk_B^*, she/he researches the buyer's record corresponding with pk_B^* at $Table_B$ and sends $C, E_{pk_B^*}(X'')$ to

the judge. These are just plain text in the view of the judge. Thus the seller (or the judge) can decrypt the buyer's copy X''.

In this scheme, the seller cannot obtain proof of treachery, because the accused buyer can claim that the unauthorized copy was created by the seller. After all, [JK02] scheme is weak against conspiracy attack. Of course, [JK02] assumes that the watermark certification authority and the judge are TTP and do not collude with a seller. But in principle, in the model for anonymous protocol the trust in the authority should be minimal. Note that when talking about attackers we also mean collusions of sellers and watermark certification authority and the judge. In other words, the seller must be able to execute all processes securely without compromising her private key even if the attacker is a trust center.

2.2.2 Observations on Efficiency

[JK02] is based on public key encryption schemes with homomorphic property [MW01] and a verifiable encryption schemes [CD98]. It presupposes additional condition as existence of the secure verifiable encryption scheme compared with [MW01] ([MW01] is based on the public key encryption schemes with homomorphic property and Cox's algorithm [CK97]). In [JK02], a verifiable encryption scheme is used in order to carry out identification protocol without any help of the accused buyer. But, a verifiable encryption scheme must take some care needs such as the secure hash function etc., [CD98] to avoid that one party falsely accuses the other of cheating.

The next undesirable point is protection of the buyer's anonymity. Most of anonymous protocols minimize the possibility of a buyer's real ID's exposure using a method: the pseudonym of a buyer is only known to an authority (normally registration center - watermark certification authority in [JK02]). But in this protocol, both the watermark certification authority and the judge can know the buyer's real ID corresponding with the buyer's anonymous public key. Besides, the judge of [JK02] scheme should be restricted. The judge that buyers chose in the watermark generation protocol must take part in identification protocol in order to identify a copyright violator. In Comparison with other anonymous protocols (Whoever is honest can be an arbiter), [JK02] scheme is inefficient in this aspect.

3 Cryptographic Primitive

3.1 Commutative Cryptosystems

We introduce the commutative cryptosystem in order to prevent the collusion of the seller and the watermark certificate center. In our protocol, even if the watermark certification authority issues the buyer's unique watermark, he/she cannot know which watermark is the buyer's one. We briefly describe the commutative cryptosystems introduced by Zhao and Varadharajan [ZV03][3] in the following.

---

[3] Commutative cryptosystems are often used in mental poker game [GM82][ZV03]. The hard part of mental poker is dealing the cards. Hands must be random and disjoint, and players

There are two parties Alice and Bob and they use the same prime number p. They have

$$K_A = \{(p, \alpha_A, k_A, \beta_A) : \beta_A \equiv {\alpha_A}^{k_A} (\text{mod } p)\}$$
$$K_B = \{(p, \alpha_B, k_B, \beta_B) : \beta_B \equiv {\alpha_B}^{k_B} (\text{mod } p)\}$$

Encryption

The original message is x. Alice chooses random value number r_A, and the result of encryption with K_A has two parts y_{1A} and y_{2A}: $E_{K_A} = (y_{1A}, y_{2A})$.

$$y_{1A} \equiv {\alpha_A}^{r_A} (\text{mod } p), y_{2A} \equiv x{\beta_A}^{r_A} (\text{mod } p)$$

Bob chooses random value number r_B, and encrypts the ciphertext of Alice's encryption and gets the following two parts: $E_{K_B} = (y_{1B}, y_{2AB})$.

$$y_{1B} = {\alpha_B}^{r_B} (\text{mod } p), y_{2AB} = x{\beta_A}^{r_A}{\beta_B}^{r_B} (\text{mod } p)$$

Actually, there is no difference whether Alice or Bob encrypts first; it will get the same ciphertext y_{1A}, y_{1B}, y_{2AB}.

Decryption

If Alice uses her private key to decrypt first,

$D_{K_A}(y_{1A,}, y_{2AB}) = y_{2AB}({y_{1A}}^{k_A})^{-1} = y_{2B} (\text{mod } p)$, and then Bob uses his private key to decrypt $D_{K_B}(y_{2B}) = y_{2B}({y_{1B}}^{k_B})^{-1} = x (\text{mod } p)$

x is the original message. Actually there is no difference whether Alice or Bob decrypts first; it could use the following formula to express the whole multi-party decryption.

$$D_{K_A,K_B}(y_{1A,}, y_{1B}, y_{2AB}) = y_{2AB}({y_{1A}}^{k_A})^{-1}({y_{1B}}^{k_B})^{-1} = x (\text{mod } p)$$

Application: Card Dealing of Mental Poker game

(1) Alice (a card dealer) encrypts original cards with her secret key one by one. The set of encrypted cards is $\{E_A(1), \cdots, E_A(52)\}$ and she sends them to Bob.

(2) Bob choose 5 cards at random say, $\{E_A(3), E_A(13), E_A(23), E_A(24), E_A(25)\}$, encrypts them. And he sends the $\{E_{AB}(3), E_{AB}(13), E_{AB}(23), E_{AB}(24), E_{AB}(25)\}$ back to Alice.

(3) Alice decrypts each element of the set, and sends the resulting set, $\{E_B(3), E_B(13), E_B(23), E_B(24), E_B(25)\}$, back to Bob.

(4) Bob decrypts the set to get his hand $\{3,13,23,24,25\}$.

In next section, we apply card dealing method that used [ZV03] scheme to watermark generation protocol.

---

should be able to claim to have any cards but those dealt. Here, the power of commutative cryptosystems is utilized. The advantage of [ZV03] is that there is no information leakage and we can extend to multi-party encryption and decryption system without losing generality because the final ciphertext is the same even if a different order is used for encryption.

4 Proposed Buyer-Seller Watermarking Protocol

In this section, we describe buyer-seller watermarking protocol without trusted third party, which is a modified scheme of [JK02] such that the watermark certification authority issues a buyer's unique watermark upon request and the encrypted watermark with the buyer's anonymous public key is received. Our scheme is based on [MW01] scheme as embedding method and [CK97] scheme as building block for collusion resistance.

4.1 Preliminary

[Preprocessing]

Let $p(\leq n\ bits)$ be a large prime such that $q = (p-1)/2$ is also a prime. Let G be a group of order $p-1$, and let g be a generator of G such that computing discrete logarithms to the base g is difficult.

[Roles of Each entity]

The entities of our scheme consist of the watermark certification authority, seller, buyer, and an arbiter. The role (or notation) of each entity is as follows.

Watermark certification authority
- Carol is short for the watermark certification authority.
- She issues watermark to buyers upon request and certify it.

Arbiter
- He/she should be convinced in trials.
- It should be possible to convince anyone as long as they know a few specific public keys.

Seller
- She (Alice) is the agent selling the contents.

Buyer
- He (Bob) is the buyer that can buy contents anonymously.

All participants (Alice, Bob, and Carol) have a pair of a secret key and a public key $(sk, pk) : [(sk_A, pk_A), (sk_B, pk_B), (sk_C, pk_C)]$ such that $pk = g^{sk} \bmod p$, all of which have been registered with appropriate certificate authority (CA).

[Notations]

We assume that the content being sold is a still image, though in general the protocol is also applicable to audio and video data like [MW01] scheme and [JK02] scheme for ease of exposition. We establish some notation as follows.

- X : Original image to be a vector of "features", $X = \{x_1, \cdots, x_m\}$.
- W : Watermark as a vector of "watermark elements", $W = \{w_1, \cdots, w_n\}$.
- X', X'' : Watermarked image

- $X \oplus W = \{x_1 \oplus w_1, \cdots, x_n \oplus w_n, x_{n+1}, \cdots, x_m\}$, $m \geq n$
- $\oplus$: Insertion operation
- E_H / D_H : Encryption/decryption algorithm with homomorphic property
- E_T / D_T : Encryption/decryption algorithm with property of commutative cryptosystem

The proposed protocol consists of the following steps: Watermark generation step for generation of a buyer's unique and valid watermark, watermark insertion step for making a watermarked content of buyers, copyright violator identification step in order to identify dishonest buyers. We introduced two cryptosystems such as cryptosystems with homomorphic property and commutative property in order that the watermark certification authority cannot know which watermark the buyer chose and sellers can embed valid watermark into content without disclosing it.

STEP 1. Watermark Generation

1. Bob chooses secret random sk^*_{B1}, sk^*_{B2} in Z_p such that $sk^*_{B1} \cdot sk^*_{B2} = sk_B \in Z_p$. Bob sends pk_B, pk^*_B $(pk^*_B = g^{sk^*_{B1}})$ and sk^*_{B2} $(E_{H\,pk_C}(sk^*_{B2}))$ encrypted by using the Carol's public key pk_C. Bob convinces Carol of zero-knowledge of possession of sk^*_{B1}. The proof given in [Ch87] for showing possession of discrete logarithms may be used here.
2. Carol first decrypts $E_{H\,pk_C}(sk^*_{B2})$ using his private key sk_C and checks that $pk^{*\,sk^*_{B2}}_B = pk_B \pmod p$ with the Bob's public key pk_B certified by CA. If it is verified, then Carol issues $k(\geq 2)$ watermarks $(W_1, W_2, \cdots, W_k)$ as follows.
   (1) Carol generates valid k watermarks $(W_1, W_2, \cdots, W_k)$ randomly. Note that $W_i = \{w_{i1}, w_{i2}, \cdots, w_{in}\}$

   Remark 1: Here, the watermark certification authority issues k watermarks, where Bob would choose one out of k watermarks. The choice of k implies a trade off between correctness and efficiency. In such case, probability that watermark certification authority can know watermark that a buyer chose would be equal to $1/k$. We use a specific construction which introduced a spread-spectrum watermarking techniques[4] proposed by Cox et al [CD98]. Each W_i of this protocol and W of Cox scheme has the same property.

   (2) Carol makes k pair $(P_1, \cdots, P_k)$ of watermarks and its signature as equation (1). First she encrypts each watermark (W_i) with Bob's anony-

[4] Cox et al., embed a set of independent real numbers $W = \{w_1, \cdots, w_n\}$ drawn from a zero mean, variance 1, Gaussian distribution into the m largest DCTAC coefficients of an image. Results reported using the largest 1000 AC coefficients show the technique to be remarkably robust against various image processing operations and after printing and rescanning and multiple-document (collusion) attack.

mous public key pk_B^*, along with a digital signature $sign_{sk_C}(E_{H\,pk_B^*}(W_i)), i = \{1,2,\cdots,k\}$ that certifies the validity of the watermarks and also ensures that pk_B^* was used to encrypt the watermark as a public key. Then she generates a pair of key (r_C, r_C') and encrypts each $P_1,\cdots,P_k$ with it using encryption scheme E_T. Here r_C is the encryption key and r_C' is a decryption key corresponding with r_C. She sends them $(EP_1,\cdots,EP_k)$ to Bob.

$$\begin{gathered} ew_1 = E_{H\,pk_B^*}(W_1),\cdots,ew_k = E_{H\,pk_B^*}(W_k) \\ s_1 = sign_{sk_C}(ew_1 \,\|\, pk_B^*),\cdots,s_k = sign_{sk_C}(ew_k \,\|\, pk_B^*) \\ P_1 = (ew_1 \,\|\, s_1),\cdots,P_k = (ew_k \,\|\, s_k) \\ EP_1 = E_{T\,r_C}(P_1),\cdots,EP_k = E_{T\,r_C}(P_k) \end{gathered} \tag{1}$$

3. Now, Bob cannot know the hidden watermark and its signature $(P_1,\cdots,P_k)$ because $(EP_1,\cdots,EP_k)$ are encrypted with Carol's secret key. Bob generates a pair of key (r_B, r_B'). r_B is encryption key and r_B' is a decryption key corresponding with r_B. He chooses one among them, $(EP_1,\cdots,EP_k)$. Suppose Bob chose $EP_3 = E_{T\,r_C}(P_3) = E_{T\,r_C}(ew_3 \,\|\, s_3)$. He encrypts it with r_B using encryption scheme E_T. He sends $E_{T\,r_B}(EP_3)$ it back to Carol.

$$E_{T\,r_B}(EP_3) = E_{T\,r_B}(E_{T\,r}\ (ew_3 \,\|\, s_3)) \tag{2}$$

4. Carol computes equation (3) and records pk_B, pk_B^* at his table $Table_C$. Then she sends $E_{T\,r_B}(ew_3 \,\|\, s_3)$ back to Bob. She is not able to know which watermark Bob chose because $(P_1,\cdots,P_k)$ is re-encrypted with Bob's secret key. Here, information to be sent to Bob is encrypted with only Bob's secret key.

$$D_{T\,r_C'}\{E_{T\,r_B}(EP_3)\} = D_{T\,r_C'}\{E_{T\,r_B}(E_{T\,r_C}(P_3)\} = E_{T\,r_B}(P_3) = E_{T\,r_B}(ew_3 \,\|\, s_3) \tag{3}$$

5. Bob decrypts $E_{T\,r_B}(ew_3 \,\|\, s_3)$ with r_B' and verifies s_3, ew_3 with Carol's public key pk_C and his secret key sk_{B1}^*.

STEP 2. Watermark Insertion

This is a two-party protocol between Alice and Bob, which proceeds as follows. From here, we will write simply ew, s rather than ew_i, s_i (in the watermark generation protocol, (ew_3, s_3)) that Bob chose.

1. Bob sends ew, s, pk_B^* to Alice.
2. Alice verifies s in order to be assured that ew is indeed a valid watermark verified by the watermark certification authority. If the verification holds,
3. Alice generates a unique watermark for this transaction V, which she inserts into the image X to get the watermarked image X'. Let X denote the image that Bob wants to purchases from Alice. The purpose of the watermark V is to

enable Alice to identify the specific user an illegal copy has potentially arisen from. She then generates a random permutation σ of degree n which she uses to permute the elements of the encrypted watermark $E_{H\,pk_B^*}(W)$ received from Bob. Alice computes $\sigma(E_{H\,pk_B^*}(W)) = E_{H\,pk_B^*}(\sigma(W))$.

4. Alice inserts the second watermark into the already watermarked image X'. Although the watermarks received from Bob is encrypted with Bob's anonymous public key pk_B^*, Alice can embed this second watermark without decrypting $E_{H\,pk_B^*}(W)$. Inserting a watermark in the encrypted domain is possible as we mention that the public key cryptosystems being used is a privacy homomorphism with respect to $\oplus$, the operation that inserts a watermark in the image. That is, Alice computes as follows

$$\begin{aligned} E_{H\,pk_B^*}(X'') &= E_{H\,pk_B^*}(X') \oplus \sigma(E_{H\,pk_B^*}(W)) \\ &= E_{H\,pk_B^*}(X') \oplus E_{H\,pk_B^*}(\sigma(W)) = E_{H\,pk_B^*}(X \oplus V \oplus \sigma(W)) \end{aligned} \tag{4}$$

5. Alice transmits $E_{H\,pk_B^*}(X'')$ to Bob and stores pk_B^*, V, σ, s, ew in her table $Table_A$. $Table_A$ is a table of records maintained by Alice for image X containing one entry for each copy X that she sells.
6. Bob decrypts $E_{H\,pk_B^*}(X'')$ with his secret key sk_{B1}^*.

$$D_{H\,sk_{B1}^*}(E_{H\,pk_B^*}(X'')) = X'' = X' \oplus \sigma(W) = X \oplus V \oplus \sigma(W) \tag{5}$$

Now Bob has a watermarked copy X'' of X that Alice cannot reproduce because she does not know the corresponding private key sk_{B1}^* and W even if she collude with Carol. Also, since Bob does not know σ, he cannot remove $\sigma(W)$ from X'', neither can he remove V which is also unknown to him.

STEP 3. Copyright Violator Identification

On discovering an unauthorized copy of X, say Y, Alice can determine the buyer from whom this copy has originated by detecting the unique watermark that she inserted for each buyer. This is done by means of a watermark extraction function and depends on the watermarking algorithm.

1. When an illegal copy Y of an original image is found, Alice extracts the unique watermark U in Y.
2. For robust watermarks, by computing correlations of extracted watermark U and every watermark stored in $Table_A$, Alice finds V with the highest correlation and obtains the transaction information involving V from the table. If U cannot be matched to any watermark V of the $Table_A$, then this protocol returns failure. Once this V is located in $Table_A$, she reads the buyer's anonymous public key pk_B^* and σ, s, ew. Alice sends them to an arbiter (judge).

3. The judge first verifies $s = sign_{sk_C}(E_{H\,pk_B^*}(W) \| pk_B^*)$ and asks Carol for real identity of an anonymous buyer. The judge would then ask Bob for his private key sk_{B1}^* which he can compute W and check for the presence of $\sigma(W)$ in Y. Actually, Bob needs not reveal his private key sk_{B1}^* because this is undesirable. He could just reveal W to the judge by decrypting $E_{H\,pk_B^*}(W)$. The judge could then verify W by encrypting it with Bob's anonymous public key and checking if it equals to $E_{H\,pk_B^*}(W)$. After verifying W, the judge can then run the watermark extraction algorithm on Y and check if $\sigma(W)$ is indeed present in Y. If $\sigma(W)$ is found in Y, Bob is found guilty otherwise he is innocent.

5 Features and Security Analysis

We discuss and analyze features and security of the proposed scheme according to the list of requirements (Section 1). We assume that all of the underlying primitives are secure. Security of our scheme relies on that of the underlying watermarking algorithm and cryptosystems.

1. **Anonymity**: We assume that the watermark certification authority does not reveal the buyer's real ID if the buyer is honest. In watermark insertion step, the seller knows ew, s, pk_B^*. Finding pk_B would require knowledge of sk_{B2}^*. However, if the encryption algorithm is secure in watermark insertion step, the only way for the seller to find sk_{B2}^* is to compute $\log_g pk_B^*$. But polynomial algorithm proving discrete logarithm problem does not exist, so attacker does not compute sk_{B2}^*. Thus buyer anonymity is guaranteed.
2. **Unlinkability**: Because our scheme executes one-time watermark generation protocol by using an anonymous key pair whenever the buyer buys a contents. This implies that the buyer's purchases are unlinkable.
3. **Traceability**: Due to the properties of the underlying encryption and digital signature techniques, we can assume that a malicious buyer cannot change or substitute a fingerprint generated by the watermark certification authority. The security of traceability is the same as that of [MW01][JK02]. Sellers should insert a watermark V and $\sigma(W)$ in the right manner for her own interest. If she does not correctly insert V, she would not be able to identify the original buyer of an illegal copy. Further a detecting function in the watermark detection must guarantees that the seller can extract the unique watermark W that belongs to a copyright violator. Besides, the buyer cannot remove $\sigma(W)$ from X'' because he does not know σ. Thus the buyer who has distributed digital contents illegally can be traced in our scheme.
4. **No Framing**: Since, to forge Y with the special watermark W, the seller must know either the buyer's private key sk_{B1}^* or the buyer's unique watermark W. In our proposal, only the buyer knows his secret key sk_{B1}^* and his unique watermark

W if computing discrete logarithm is hard and used encryption algorithm (underlying primitives) is secure. Since we use secure commutative cryptosystems in the watermark generation protocol, even the watermark certification authority does not know which watermark the buyer selected. Thus an honest buyer should not be wrongly identified as a copyright violator, because the others cannot recreate the buyer's copy with specific watermark.

5. **No Repudiation**: The buyer accused of reselling an unauthorized copy cannot claim that the copy was created by the seller or a security breach of the seller's system. Since only the buyer know his secret key sk_{B1}^{*} and his unique watermark W, the others cannot recreate the buyer's copy.
6. **Collusion Tolerance**: Our scheme has used [CK97] as a building block. We assumed that this algorithm is secure. And this algorithm is estimated to be highly resistant to collusion attacks [KT98]. Our protocol is secure only as much as the underlying watermarking techniques are secure and robust.
7. **Security against conspiracy attack**: To success in conspiracy attack, seller and the watermark certification authority must know either the watermark W or the buyer's secret key sk_{B1}^{*}. But in our scheme, no one (except the buyer) knows the buyer's unique watermark W and secret key sk_{B1}^{*}. And our protocol is secure against conspiracy attack because the judge of our scheme does not take part in others step except identification step (The arbiter knows just a specific public key). Thus our scheme does not need any trusted third party because all participators' dishonesty can be controlled.

6 Concluding Remarks

To protect both seller and buyer's rights and buyer's anonymity, [JK02] proposed "an anonymous buyer-seller watermarking protocol". But the problem of this protocol is that sellers can recreate the buyer's copy if he/she colludes with the watermark certification authority and the judge. Thus [JK02] scheme must need the trusted third parties for its security. On the contrary, we propose secure buyer-seller watermarking protocol without trusted third party. For it, we apply secure commutative cryptosystems to watermarking protocol. But, drawbacks of our scheme compared with [JK02] are that it requires high computational complexity and communication pass number in watermark generation step. A further direction of this study will be to diminish computational complexity.

References

[BS95] D.Boneh and J.Shaw, "Collusion-secure Fingerprinting for Digital Data", Crypto'95, LNCS 963, Springer-Verlag, 1995, pp. 452–465.

[CD87] D.Chaum, Ivan Bjerre Damgard and Jeroen van de Graaf., "Multiparty Computation Ensuring Privacy of Each Party's Input and Correctness of the Result", Crypto'87, LNCS 293, Springer-Verlag, 1987, pp. 86–119.

[CD98] J.Camenisch and I.Damgard, "Verifiable encryption and applications to group signatures and signatures sharing", Technical Report RS 98-32, Brics, Department of Computer Science, University of Aarhus, Dec.1998.

[Ch87] D.Chaum, "An improved protocol for demonstrating possession of discrete logarithms and some generalizations", Eurocrypto'87, LNCS 304, Springer-Verlag, 1987, pp.127–141.

[CK97] I.J. Cox, J.Kilian, T.Leighton, and T.Shamnon, "Secure spread spectrum watermarking for image, audio and video", IEEE Transactions on Image Processing, vol.6, no 12, pp.1673–1678, 1997.

[GM82] Goldwasser, S. and Micali, S. "Probabilistic Encryption and How to play Mental Poker Keeping Secret All Partial Information", Proceedings of the 14th STOC, pp.365–377, 1982.

[JK02] Hak-Soo Ju, Hyung-Jeong Kim, Dong-Hoon Lee and Jong-In Lim., "An Anonymous Buyer-Seller Watermarking Protocol with Anonymity Control", ICISC2002, LNCS 2587, Springer-Verlag, 2003, pp. 421–432.

[KT98] Joe Killian, F. Thomson Leighton, Lasely R. Matheson, Talal G. Shannon, Robert E. Tarjan, and Francis Zane, "Resistance of Digital Watermarks to Collusive attacke", 1998.

[Ne83] Neal.R.Wanger, "Fingerprinting", IEEE Symposium on Security and Privacy, 1983.

[MW01] N.Memon and P.W.Wong, "A Buyer-Seller Watermarking Protocol", IEEE Transactions on image processing, vol.10, no. 4, pp. 643–649, April 2001.

[PS00] B.Pfitzman and Ahmad-Reza Sadeghi, "Coin-Based Anonymous Fingerprinting", Eurocrypt'99, LNCS 1592. Springer-Verlag, 2000, pp.150–164.

[PS96] B.Pfitzman and M.Schunter, "Asymmetric Fingerprinting", Eurocrypt'96, LNCS 1070, Springer-Verlag, 1996, pp.84–95.

[PW97] B.Pfitzman and W.Waidner, "Anonymous Fingerprinting", Eurocrypto'97, LNCS 1233, Springer-Verlag, 1997, pp. 88–102.

[QN98] L.Qian and K.Nahrstedit, "Watermarking schemes and protocols for protecting rightfuk ownership and customer's rights", J.Visual Commun. Image Represent, vol. 9, pp.194–210, Sept. 98.

[ZV03] Weiliang Zhao, Vijay Varadharajan and Yi Mu, "A secure Mental Poker Protocol Over the internet", Australasian Information Security Workshop 2003. Conference in Research and Practice in Information Technology, Vol.21, 4.Feb.2003.