An Improved Anonymous Buyer-Reseller Watermarking Protocol

Fuh-Gwo Jeng[1], Jyun-Ci Huang[2], and Tzung-Her Chen[2]
(Corresponding author: Tzung-Her Chen)

Department of Applied Mathematics, National Chiayi University[1]
Department of Computer Science and Information Engineering, National Chiayi University[2]
300 University Rd., Chia-Yi City, Taiwan 60004, R.O.C.
(Email: thchen@mail.ncyu.edu.tw)
(Received June 17, 2014; revised and accepted Jan. 16 & Apr. 2, 2015)

Abstract

Although digital watermarking protocols have been studied extensively for achieving copyright protection over the Internet for many years, the new issue of second-hand watermarking protocols has been largely ignored. Cheung and Curreem first proposed a buyer-reseller watermarking protocol for digital content redistribution in the second-hand markets. Later, Chen et al. showed that Cheung and Curreem's scheme is vulnerable to malicious attacks and further proposed a simple improvement. However, in this paper, we show that the aforementioned schemes are still insecure, specifically by seller cheating problems, and propose an improved one. Moreover, the proposed scheme accounts for requirements of anonymity, unlinkability, coalition-resistance, and traitor traceability.
Keywords: Buyer-reseller, copyright protection, digital watermarking, second-hand market, watermarking protocol

1 Introduction

As life becomes more digitalized, large amounts of text, images, audio or video are digitalized and, thus, on-line transaction has drawn much attention [21]. To protect these digital contents, digital watermarking [6, 14, 15, 17] and digital watermarking protocols [13] have been proposed for solving the copyright protection problem.

Almost all proposed watermarking protocols focus on first-hand markets [2, 3, 7, 9, 10, 11, 12, 13, 16, 19]. The watermarking protocols for securing transactions of digital contents in a second-hand market have been afforded less effort despite the high potential for financial returns. There are several reasons why industry is so profitable.

First, buyers are willing to purchase second-hand digital contents because of lower prices and identical quality. Second, the second-hand environment welcomes resellers. Third, sellers are willing to accept the market discipline and join the second-hand market if they can benefit sufficiently from transactions.

The key difference between a traditional second-hand market and the digital second-hand market is whether or not the reseller can keep a copy. In a traditional second-hand market, if the reseller sells the content, (s)he no longer owns the content anymore. However, in a digital second-hand market, if the reseller sells the content, (s)he may still have a private copy. Then, (s)he may have the opportunity to redistribute the copy. Therefore, in a second-hand market for digital content, we not only need to consider the rights and illegal redistribution between the seller and the buyer, but also the reseller.

Taking second-hand scenarios into account, the following requirements must be met:

Asymmetry: In a secure watermarking protocol, the buyer is the only one who is both aware of and also possesses the watermarked digital content. Therefore, if an illegal copy is found, the seller can trace the identity of the buyer who distributed the copy and prove to the judge that the buyer is guilty of illegal distribution. On the other hand, the buyer cannot deny charge by claiming that the unauthorized copy was distributed by the seller, or the reseller.

Anonymity: If requested, the identity of a buyer should not be exposed unless (s)he is confirmed to be an illegal distributor.

Malicious insiders (seller, buyer and reseller): A malicious insider may intend to benefit from reselling unauthorized copies by means of the following cases.

1) If the seller intends to cheat a buyer, (s)he may distribute a watermarked copy that has already been sold to the buyer.
2) The reseller may intend to benefit from reselling unauthorized copies.

Table 1: The notations used in this paper

B, S, R, CA, J:	A buyer, seller, reseller, watermark certification authority and the judge, respectively;
ID_B:	Identity of **B**;
$X' = X \oplus W$:	Embeds watermark W into original content X to form watermarked content X';
V_B, V_R:	The watermarks indicating the transactions from the buyer and reseller;
B $\rightarrow$ **S**: M:	**B** delivers message M to **S**;
$E_k(.), D_s(\cdot)$:	The encryption function with the public key k and decryption function with the private key s;
$H(\cdot)$:	A one-way hash function;
$Sign_s(M)$:	Digital signature of message M signed by the private key s.

3) The buyer may claim that the unauthorized copy was resold by the seller, or the reseller.

Unlinkability: Sellers and resellers cannot determine whether any two transactions belong to the same buyer or not.

Coalition resistance: Two or more buyers cannot cooperate to obtain another buyer's transaction information.

Traitor traceability: When a pirated copy is found, it must be easy to distinguish who is the traitor.

Inspired by Memon and Wong's scheme, Cheung and Curreem [5] proposed a buyer-reseller watermarking protocol (hereby shortened to CC) for digital contents redistributing in digital second-hand market. Later, Chen et al. [4] showed that the CC scheme is still susceptible to seller cheating and reseller cheating problems. Chen et al. then proposed an improved one (hereby shortened to CHT) with anonymity.

In this paper, we will show that both of the CC and the CHT schemes, which violate the asymmetry requirement, are not immune to the seller cheating problem and an enhanced one is proposed. Thanks to the tool of commutative cryptosystem, the reseller's watermarked content can be encrypted before transmitting to the seller. In this way, the seller is not aware of the reseller's watermarked content and the seller cheating problem can be solved. Naturally, the proposed protocol also satisfies all above precautionary requirements.

2 Review and Security Analysis of the CC and the CHT Schemes

In this section, the CHT scheme is briefly reviewed while the CC scheme is similar and, thus, omitted. Table 1 gives the notations used through this paper.

To begin with, the kernel technique of watermarking protocol should be mentioned. Memon and Wong's watermarking protocol adopts a public key cryptosystem that is a privacy homomorphism with respect to the watermark insertion operator. Here, the watermark insertion operation is $X \oplus W = \{x1 \oplus w1, x2 \oplus w2, \cdots, xm \oplus wm, xm+1 \oplus wm+1, \cdots, xn \oplus wn\}$ and $\oplus$ is a privacy homomorphism with respect to a binary operator for the public-key cryptosystem. It is well-know that the RSA cryptosystem is a privacy homomorphism with respect to multiplication. Precisely, $Ek(a \oplus b) = Ek(a) \oplus Ek(b)$ is hold where a and b are in the message space. A specific construction by combining the well-known spread-spectrum watermarking technique proposed by Cox et al. [6] and the RSA cryptosystem is given in [13] with respect to multiplication.

2.1 Review of the CHT Scheme

2.1.1 Registration Protocol

The buyer **B** asks for a temporary transaction key pair from **CA**. **CA** generates a short-term key pair (pk_B^*, sk_B^*) and a watermark W for **B**. Then **CA** sends them to the buyer securely.

1) **B** $\rightarrow$ **CA:** A certificate of **B**'s identity including the public key pk_B.
CA verifies the validation of **B**'s identity and pk_B by checking the certificate.

2) **CA** $\rightarrow$ **B:** $E_{pk_B}((pk_B^*, sk_B^*), E_{pk_B^*}(W), Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*))$.
CA generates a watermark W and the temporary key pair (pk_B^*, sk_B^*), and computes $Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$ and $E_{pk_B}((pk_B^*, sk_B^*), E_{pk_B^*}(W), Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*))$ where sk_{CA} is CA's private key.

3) **B** decrypts the received message and checks the validity of $Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$. **CA** also stores ID_B and pk_B^* in the table.

2.1.2 Watermark Insertion Protocol

The reseller **R** may designate a transaction proxy, for example an auction web site, and the buyer directly communicates with the transaction proxy via the Internet.

1) **B** → **R:** $E_{pk_B^*}(W), pk_B^*, Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$.
The buyer **B** sends the message $\{E_{pk_B^*}(W),\ pk_B^*,\ Sign_{sk_{CA}}(E_{pk_B^*}(W),\ pk_B^*)\}$ to the reseller **R**.

2) **R** → **S:** $E_{pk_B^*}(W), pk_B^*, Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*), X_R$.
R forwards the message $\{E_{pk_B^*}(W),\ pk_B^*,\ Sign_{sk_{CA}}(E_{pk_B^*,pk_B^*}),\ X_R\}$ to the seller **S** where X_R is the content that **B** intends to buy.

3) **S** extracts V_R from X_R and searches V_R in the database. If V_R does not exist, X_R is not a legal copy of **R**; otherwise, **S** checks the validity of $E_{pk_B^*}(W)$ by verifying $Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$ with **CA**'s public key. If it fails, the operation is terminated; otherwise, **S** performs the following operations.

   - **S** generates a new transaction watermark V_B to denote this transaction, where V_B is embedded into X_R to form $X_B = X_R \oplus V_B$.
   - **S** generates a random permutation function $p_B(.)$ and computes
   $$p_B(E_{pk_B^*}(W)) = E_{pk_B^*}(p_B(W)).$$
   - **S** computes
   $$E_{pk_B^*}(X_B') = E_{pk_B^*}(X_B) \oplus E_{pk_B^*}(p_B(W)).$$
   - **S** stores $E_{pk_B^*}(W), pk_B^*, V_B, Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*), p_B(.)$ in the database and transfers R's ownership from the database to another reselling database.

4) **S** → **R:** $E_{pk_B^*}(X_B'), M, Sign_{sk_S}(M, pk_R^*)$.
S sends the message $E_{pk_B^*}(X_B'), M, Sign_{sk_S}(M, pk_R^*)$ to **R** where M indicates this reselling transaction and pk_R^* denotes the reseller's short-time public key already stored in the database before and sk_S is **S**'s private key. Then the reseller verifies $M, Sign_{sk_S}(M, pk_R^*)$ and keeps them as a certificate.

5) **R** → **B:** $E_{pk_B^*}(X_B')$.
R sends $E_{pk_B^*}(X_B')$ to **B**.

6. **B** decrypts $E_{pk_B^*}(X_B')$ to obtain $X_B' = X_B \oplus p_B(W)$ with the private keys sk_B^*.

2.1.3 Dispute Resolution Protocol

If an unauthorized copy Y is found by **S**, **S** extracts the transaction watermark V_B or V_R and searches the database to retrieve pk_B^* or pk_R^*. If only V_R is found, **R** is sued. If both V_B and V_R are found, **B** is sued. Then **CA** is requested to reveal who owns pk_B^* (or pk_R^*). The following is an example if both V_B and V_R are found.

1) **S** → **J:** $E_{pk_B^*}(W), pk_B^*, V_B, Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$, and $p_B(.)$.
S sends the message $\{E_{pk_B^*}(W),\ pk_B^*,\ V_B,\ Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*),\ p_B(.)\}$ to **J**.

2) **J** verifies the validity of $Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$, then computes, $E_{pk_B^*}(Y), E_{pk_B^*}(p_B(W))$ and finally checks whether $E_{pk_B^*}(p_B(W))$ exists in $E_{pk_B^*}(Y)$ or not. If it is found, **B** is convicted guilty; otherwise, (s)he is innocent. Finally, **J** asks **CA** to show the identity of the buyer who owns pk_B^*.

2.2 Security Analysis

Both of the CC and the CHT schemes are vulnerable to the seller cheating problem. In the watermark insertion protocols of the CC and the CHT schemes, the reseller **R** needs to return the copy X_R to the seller **S**. Once **S** obtains X_R, (s)he can illegally distribute X_R or sell X_R to other buyers, so called the seller cheating problem [4]. Because the digital content X_R still contains the watermark of **R**, **R** will be potentially sued in the dispute resolution protocol if an unauthorized copy Y of X_R is found by **S**. Neither the CC scheme nor the CHT scheme accounted for this problem. Specifically, the buyer-reseller watermarking protocols in the literature do not guarantee asymmetry property. To this end, we will propose an enhanced scheme to prevent **S** from obtaining **R**'s copy X_R.

3 The Proposed Scheme

Prior to describing the proposed scheme, the preliminary, commutative cryptosystem adopted in [18], is introduced to prevent seller cheating problems which exist in both of the CC and the CHT schemes.

3.1 Commutative Cryptosystem

Commutative cryptosystems are often used in mental poker games [20]. The basic concept is that the encryption and decryption order does not matter if some secret messages needed to be encrypted and decrypted twice or more, respectively.

A cryptosystem E is said to be commutative if it satisfies the following property: for any two keys K_1 and K_2 and any message m, $E_{K_1}(E_{K_2}(m)) = E_{K_2}(E_{K_1}(m))$ and $D_{K_2}(E_{K_1}(E_{K_2}(m))) = E_{K_1}(m)$, where $D(.) = E^{-1}(.)$.

An example [8] of ElGamal-type commutative cryptosystem is given below. Assume two parties, Alice and Bob, have

$$\begin{aligned} K_A &= (p, g_A, x_A, y_A) : y_A = g_A^{x_A} (mod\ p) \\ K_B &= (p, g_B, x_B, y_B) : y_B = g_B^{x_B} (mod\ p), \end{aligned}$$

where x_A and y_A (x_B and y_B) are the private and public key pair of Alice (Bob).

Encryption.

To encrypt a message m, Alice first chooses a random value number r_A and computes the ciphertext $C_A = (C_{A1}, C_{A2})$, where

$$\begin{aligned} C_{A1} &= g_A^{r_A} \bmod p, \\ C_{A2} &= m * y_A^{r_A} \bmod p. \end{aligned}$$

Bob chooses a random value number r_B and encrypts Alice's ciphertext C_A to obtain $C_B = (C_{B1}, C_{AB})$, where

$$\begin{aligned} C_{B1} &= g_B^{r_B} \bmod p, \\ C_{AB} &= m * y_A^{r_A} * y_B^{r_B} \bmod p. \end{aligned}$$

In reality, whether Alice or Bob does the encryption operation first will not affect the result, $C = (C_{A1}, C_{B1}, C_{AB})$.

Decryption.

Suppose Alice uses her private key to decrypt first, i.e.

$$\begin{aligned} C' &= C_{AB} * (C_{A1}^{x_A})^{-1} \\ &= m * y_B^{r_B} mod\ p. \end{aligned}$$

Then Bob uses the private key to decrypt, where

$$C' * (C_{B1}^{x_B})^{-1} = m \bmod p.$$

The result will not be affected by whether Alice or Bob does the operation first.

3.2 Registration Protocol

The registration protocol is the same as that in Section 2.1.1. Therefore, it is omitted here.

3.3 Watermark Insertion Protocol

The reseller may designate a transaction proxy, for example an auction web site, and the buyer directly communicates with the transaction proxy using a MIX network [1] via the Internet. Note that the watermarking insertion requires a privacy homomorphism such as RSA-based cryptosystem mentioned in Section 2.

1) **B** $\rightarrow$ **R:** $E_{pk_B^*}(W), pk_B^*, Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$.
The buyer **B** sends the message $\{E_{pk_B^*}(W),\ pk_B^*,\ Sign_{sk_{CA}}(E_{pk_B^*}(W),\ pk_B^*)\}$ to the reseller **R**.

2) **B** $\rightarrow$ **R:** $E_{pk_B^*}(W), pk_B^*, Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$, $E_{pk_R^*}(X_R), AGR, Sign_{sk_R^*}(AGR \parallel E_{pk_R^*}(X_R))$.
R first negotiates with **S** to set up a common agreement, AGR, which explicitly states the ownership transfer rights and obligations from **R** to **B** of X_R. Then (s)he computes $E_{pk_R^*}(X_R)$ and $s_1 = Sign_{sk_R^*}(AGR \parallel E_{pk_R^*}(X_R))$, where pk_R^* denotes the reseller's short-time public key already stored in the database before.

3) After receiving **R**'s message, **S** performs the following operations.

- **S** verifies the signature $s_1 = Sign_{sk_R^*}(AGR \parallel E_{pk_R^*}(X_R))$ for checking whether the messages are sent from **R**. If yes, (s)he computes the message authentication code (MAC) value $m' = H(E_{pk_R^*}(X_R), pk_R^*)$.
- **S** uses pk_R^* as a keyword and searches the record of pk_R^*. From the matched record, (s)he selects m and checks if m is equal to the computed m' or not where $m = H(E_{pk_R^*}(X_R), pk_R^*)$ is computed in the first-hand transaction. If not, X_R is not a legal copy of **R**. Otherwise, **S** checks the validity of $E_{pk_B^*}(W)$ by verifying $Sign_{sk_{CA}}(E_{pk_B^*}(W), pk_B^*)$ with **CA**'s public key. If it fails, **S** terminates the transaction.
- **S** generates a new transaction watermark V_B which is embedded into X_R, to denote this transaction to get X_B, precisely,

$$\begin{aligned} & E_{pk_B^*}(E_{pk_R^*}(X_B)) \\ = \ & E_{pk_B^*}(E_{pk_R^*}(X_R)) \oplus E_{pk_B^*}(E_{pk_R^*}(V_B)). \end{aligned}$$

- **S** generates a random permutation function $p_B(.)$ and computes

$$p_B(E_{pk_B^*}(E_{pk_R^*}(W))) = E_{pk_B^*}(E_{pk_R^*}(p_B(W))).$$

- **S** computes $E_{pk_B^*}(E_{pk_R^*}(X'_B))$ and the new MAC value m as follows.

$$\begin{aligned} & E_{pk_B^*}(E_{pk_R^*}(X'_B)) \\ = \ & E_{pk_B^*}(E_{pk_R^*}(X_B)) \oplus E_{pk_B^*}(E_{pk_R^*}(p_B(W))) \end{aligned}$$

and

$$m = H(E_{pk_B^*}(E_{pk_R^*}(X'_B)), pk_B^*).$$

- **S** stores $E_{pk_B^*}(W)$, pk_B^*, m, V_B, $Sign_{sk_{CA}}(E_{pk_B^*}(W),\ pk_B^*)$, and $p_B(.)$ in the database; transfers R's ownership from the database to another reselling database.
- **S** generates M and $Sign_{sk_s}(M, pk_R^*)$, where M indicates this reselling transaction.

4) **S** $\rightarrow$ **R:** $E_{pk_B^*}(E_{pk_R^*}(X'_B)), M, Sign_{sk_S}(M, pk_R^*)$.
S sends the message $\{E_{pk_B^*}(E_{pk_R^*}(X'_B)),\ M,\ Sign_{sk_S}(M, pk_R^*)\}$ to **R**.

5) **R** $\rightarrow$ **B:** $E_{pk_B^*}(X'_B)$.
R computes $D_{sk_R^*}(E_{pk_B^*}(E_{pk_R^*}(X'_B))) = E_{pk_B^*}(X'_B)$ and verifies M by checking the validation of $Sign_{sk_S}(M, pk_R^*)$ and keeps them as a certificate. Then, **R** sends $E_{pk_B^*}(X'_B)$ to **B**.

6) **B** decrypts $E_{pk_B^*}(X'_B)$ to obtain $X'_B = X_B \oplus p_B(W)$ with the private key, sk_B^*.

3.4 Dispute Resolution Protocol

This subprotocol is the same as that in Section 2.1.3, and thus omitted here.

4 Security Analysis and Discussions

The main security problem in the buyer-reseller watermarking protocol comes from the seller-cheating problem that the seller obtains the sold copy X_R. Hence, the proposed improvement aims at avoiding this security concern by maintaining the asymmetry property. The security of the proposed buyer-reseller watermarking protocol is based on the following assumptions.

Assumption 1. *By a well-constructed MIX mechanism, the seller or an attacker gains no information about who purchased the digital content since the communication is untraceable.*

Assumption 2. *To guarantee the anonymity of buyer-reseller watermarking protocol, buyers must refresh the short-term transaction key pairs.*

First, we shall focus on how the proposed scheme can resist the seller cheating problems. Second, further discussions will be shown.

4.1 Seller Cheating Problems

Lemma 1. **S** *cannot cheat* ***B*** *by means of either reselling the watermarked copy which was sold to some buyer or impersonating a buyer to launch the transaction protocol.*

Proof. If **S** wants to cheat **B**, (s)he must obtain the watermarked content $X'_B = X_B \oplus p_B(W) = X_R \oplus V_B \oplus p_B(W)$ of **B**. However, the watermarked content X'_B is well protected by asymmetric encryption in the form of $E_{pk^*_B}(X'_B)$. Without the corresponding private key sk^*_B, **S** cannot decrypt the encrypted X'_B to obtain X'_B. Since **S** cannot obtain a watermarked content X'_B, therefore, **S** cannot illegally distribute X'_B and accuse **B** of piracy.

Furthermore, if **S** intends to impersonate **B**, (s)he faces the same problem as (s)he lacks the private key sk^*_B necessary to decrypt the watermarked content.

In sum, **S** cannot cheat **B**. □

Lemma 2. **S** *cannot cheat* ***R*** *by means of either reselling the watermarked copy which was sold to the reseller or maliciously accuse the reseller of piracy if an unauthorized copy is found.*

Proof. If **S** wants to cheat **R**, (s)he must obtain the watermarked content X_R of **R**. Since X_R is well protected by commutative cryptosystem, **S** has no efficient way to obtain X_R. Therefore, **S** cannot distribute X_R and accuse **R** of piracy.

Furthermore, **S** intends to maliciously accuse the reseller of piracy if an unauthorized copy, which was resold to a buyer but illegally redistributed by that buyer, is found. In the watermarking insertion phase, **R** keeps M and $Sign_{sk_S}(M, pk^*_R)$ as a certificate. **R** has this evidence to show (s)he is innocent. □

Theorem 1. *The proposed buyer-reseller watermarking protocol can resist the seller cheating problems.*

Proof. By **Lemmas 1** and **2**, **S** has no feasible way to cheat either **B** or **R**. Therefore, the proposed protocol can resist the seller cheating problems. □

4.2 Further Discussions

1) **Malicious Reseller.**
A malicious reseller **R** may send a fake $E_{pk^*_R}(X_R)$ to cheat **S**. Since X_R is encrypted by pk^*_R, **S** can not extract V_R. **S** can verify the validity of the received $E_{pk^*_R}(X_R)$ by comparing the computed MAC value $m' = H(E_{pk^*_R}(X_R), pk^*_R)$ and the stored value $m = H(E_{pk^*_R}(X_R), pk^*_R)$. If not identical, **S** rejects this transaction.

   Furthermore, **R** has no feasible way to frame **B**, either. Without the corresponding private key sk^*_B, **R** cannot decrypt the encrypted X'_B to obtain X'_B. Since **R** cannot obtain a watermarked content X'_B, therefore, **R** cannot illegally distribute X'_B and frame **B** later.

2) **Malicious Buyer.**
Since the seller and the reseller are unaware of the watermarked copy, the buyer cannot reasonably claim that the unauthorized copy was resold by the seller or the reseller. If **B** illegally distributes X'_B, (s)he can be traced in the way of the protocol in **Section. 3.4**.

3) **Anonymity.**
In the proposed protocol, the reseller uses a short-term key pair (pk^*_R, sk^*_R) for a transaction. During the transaction, the seller only knows a short-term public key, pk^*_R. Besides, The buyer uses a short-term key pair (pk^*_B, sk^*_B) for a transaction, too. The reseller only knows a short-term public key, pk^*_B. The seller does not know who the reseller/buyer is and the reseller does not know who the buyer is. In addition, by **Assumption 1**, the seller gains no information about who purchased the digital content. In this way, anonymity is guaranteed.

4) **Unlinkability.**
Buyers use their short-term key pairs for anonymous transaction. If a buyer reuses the short-term key pair for various transactions, some of the buyer's habits may be revealed. In the proposed protocol, both the sellers and the resellers know the triple $\{E_{pk^*_B}(W), pk^*_B, Sign_{sk_{CA}}(E_{pk^*_B}(W), pk^*_B)\}$. By **Assumption 2**, sellers and resellers cannot determine whether any two transactions belong to the same buyer or not.

5) **Coalition-Resistance.**
If two or more buyers collude (say B_1 and B_2), they still can not forge another buyer's transaction message $\{E_{pk^*_{B_3}}(W), pk^*_{B_3}, Sign_{sk_{CA}}(E_{pk^*_{B_3}}, pk^*_{B_3})\}$

Table 2: Comparison between the related schemes and the proposed scheme

Requirements	Memon-Wong [13]	Lei et al. [12]	Cheung-Currem [5]	Chen et al. [4]	The proposed
First-hand	Yes	Yes	Yes	Yes	Yes
Second-hand	No	No	Yes	Yes	Yes
Asymmetry	Yes	Yes	No*	No*	Yes
Anonymity	No	Yes	No	Yes	Yes
Unlinkability	N/A	N/A	N/A	Yes	Yes
Coalition resistance	Yes	Yes	Yes	Yes	Yes
Traitor traceability	Yes	Yes	Yes	Yes	Yes

*: Sellers might have watermarked copies sent from resellers in the second-hand scenario.

from their transaction messages $\{E_{pk^*_{B_1}}(W),\ pk^*_{B_1},\ Sign_{sk_{CA}}(E_{pk^*_{B_1}}(W),\ pk^*_{B_1})\}$ and $\{E_{pk^*_{B_2}}(W),\ pk^*_{B_2},\ Sign_{sk_{CA}}(E_{pk^*_{B_2}}(W),\ pk^*_{B_2})\}$. It goes without saying that it is not feasible to calculate the private key.

6) **Traitor Traceability.**
It is easy to distinguish who is the real traitor, since the buyer's transaction watermark is stored in the database and the reseller's transaction watermark is stored in the reselling database. The seller can distinguish who is the real illegal distributor. With the help of CA, the traitor can be traced and revealed by searching the database.

At the end of this section, Table 2 gives the further functionality comparisons between the related works and the proposed scheme. The proposed buyer-reseller watermarking protocol not only satisfies the requirements for second-hand markets which the earlier [12, 13] are not suitable for, but also provides the secure protocol compared with the other two buyer-reseller protocols [4, 5]. The traditional buyer-seller watermarking protocols [12, 13] do not support the second-hand market. The second-hand buyer-seller watermarking protocols [4, 5] are shown insecure by lacking asymmetry property.

Furthermore, Table 3 provides the comparison of computation cost. Since the computational cost of hash function is much lower than that of public-key operations, it is omitted in Table 3. In the dispute resolution subprotocol, the cost of the proposed scheme is almost the same as that of the related schemes. In the registration and watermark insertion subprotocols, they cost more than the CC and the CHT related subprotocols. The extra computation cost in the proposed protocol is mainly due to the inclusion of commutative encryption, which is adopted to enhance security for the protocol in the proposed scheme.

5 Conclusions

As the fact that a digitalized second-hand market has high commerce potential [4], researchers have rarely addressed the watermarking protocols for digitalized second-hand markets, transactions of digital contents. Although the existing CC and CHT schemes aim at this end, the authors show that the CC and CHT schemes cannot resist the seller-cheating problem. Therefore, it is worthwhile to remedy security weaknesses. Thus an improved second-hand watermarking protocol is proposed, in which all above mentioned requirements are satisfied including asymmetry, anonymity, resistance to malicious insiders, unlinkability, resistance to coalition attacks and traitor traceability.

Acknowledgments

This work was partially supported National Science Council, Taiwan, R.O.C., under contract by NSC 102-2221-E-415-014 and NSC 102-2221-E-415-007.

References

[1] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, 1981.

[2] C. L. Chen, C. C. Chen, D. K. Li and P. Y. Chen, "A verifiable and secret buyer-seller watermarking protocol," *IETE Technical Review*, pp. 1–10, 2014.

[3] T. H. Chen, G. Horng, "A lightweight and anonymous copyright-protection protocol," *Computer Standards and Interfaces*, vol. 2929, no. 2, pp. 229-237, 2007.

[4] T. H. Chen, G. Horng, and D. Tsai, "An anonymous buyer-reseller watermarking protocol," *Journal of the Chinese Institute of Engineers*, vol. 28, no. 3, pp. 535–538, 2005.

[5] S. C. Cheung and H. Currem, "Rights protection for digital contents redistribution over the internet," in *Proceedings of 26th Annual International Computer Software and Applications Conference*, pp. 105–110, 2002.

Table 3: Comparison of performance between the CC, CHT schemes and the proposed scheme for (a) registration and watermark insertion protocols and (b) dispute resolution protocol

(a)

Operation	Watermark embedding	Signing/verifying	Public-key en(de)cryption
Schemes	B/ R / S/ CA/ J	B/ R / S/ CA/ J	B/ R / S/ CA/ J
CC [5]	0 / 0 / 3 / 0 / 0	1 / 0 / 1 / 2 / 0	1 / 0 / 1 / 1 / 0
CHT [4]	0 / 0 / 3 / 0 / 0	1 / 1 / 2 / 2 / 0	2 / 0 / 1 / 2 / 0
Ours	0 / 0 / 2 / 0 / 0	1 / 2 / 2 / 2 / 0	2 / 2 / 4 / 2 / 0

(b)

Operation	Watermark extraction	Signing/verifying	Public-key en(de)cryption
Schemes	S/ J	S/ J	S/ J
CC [5]	1 / 1	0 / 1	0 / 1
CHT [4]	2 / 1	0 / 1	0 / 1
Ours	2 / 1	0 / 1	0 / 1

[6] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, pp. 1673–1687, 1997.

[7] Z. Eslami, M. Kazemnasabhaji and N. Mirehi, "Proxy signatures and buyer-seller watermarking protocols for the protection of multimedia content," *Multimedia Tools and Applications*, vol. 72, pp. 2723–2740, 2014.

[8] J. Gwi, K. Sakurai, and J. H. Park, "Does it need trusted third party? Design of Buyer-Seller watermarking protocol without trusted third party," in *Proceedings of ACNS'03*, LNCS 2846, pp. 265–279, Springer, 2003.

[9] A. Kumar, S. P. Ghrera and V. Tyagi, "A comparison of buyer-seller watermarking protocol (BSWP) based on discrete cosine transform (DCT) and discrete wavelet transform (DWT)," in *Proceedings of the 49th Annual Convention of the Computer Society of India (CSI'15)*, vol. 1, pp. 401–408, 2015.

[10] M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for on-line trade using information gap between buyer and merchant," *IEICE Transactions on Fundamentals*, vol. E89-A, no. 4, pp. 1725–1737, 2006.

[11] S. H. Lee, S. G. Kwon, and K. R. Kwon, "Mobile 3D secure transmission based on anonymous buyer-seller watermarking protocol," *Recent Advances in Communications and Networking Technology*, vol. 3, pp. 33–43, 2014.

[12] C. L. Lei, P. L. Yu, P. L. Tsai, and M. H. Chan, "An efficient and anonymous buyer-seller watermarking protocol," *IEEE Transactions on Image Processing*, vol. 13, no. 12, pp. 1618–1626, 2004.

[13] N. Memon and P. W. Wong, "A Buyer-Seller watermarking protocol," *IEEE Transactions on Image Processing*, vol. 10, no. 4, pp. 643–649, 2001.

[14] S. C. Pei, J. M. Guo, and H. Lee, "Novel robust watermarking technique dithering halftone images," *IEEE Signal Processing Letters*, vol. 12, no. 4, pp. 333–336, 2005.

[15] X. Qi and J. Qi, "A robust content-based digital image watermarking scheme," *Signal Processing*, vol. 87, no. 6, pp. 1264–1280, 2007.

[16] L. Qian and K. Nahrstedt, "Watermarking schemes and protocols for protecting rightful ownership and customer's rights," *Journal of Visual Communication and Image Representation*, vol. 9, no. 3, pp. 194–210, 1998.

[17] J. M. Shieh, D. C. Lou, and M. C. Chang, "A semi-blind digital watermarking scheme based on singular value decomposition," *Computer Standards and Interfaces*, vol. 28, no. 4, pp. 428–440, 2006.

[18] C. Wang, H. F. Leung, S. C. Cheung, and Y. Wang, "Use of cryptographic technologies for privacy protection of watermarks in internet retails of digital contents," in *Proceedings of the 18th International Conference on Advanced Information Networking and Applications*, vol. 1, pp. 414–419, 2004.

[19] S. Yong and S. H. Lee, "An efficient fingerprinting scheme with symmetric and commutative encryption," in *Proceedings of IWDW'05*, LNCS 3710, pp. 54–66, Springer, 2005.

[20] W. Zhao, V. Varadharajan, and Y. Mu, "A secure mental poker protocol over the internet," in *Proceedings of the Australasian Information Security Workshop*, vol. 21, pp. 105–109, 2003.

[21] S. F. Tzeng, M. S. Hwang, and H. B. Chen, "A secure on-line software transaction scheme," *Computer Standards and Interfaces*, vol. 27, no. 3, pp.303–312, Mar. 2005.

Fuh-Gwo Jeng received his M.S. in computer and information science from National Chiao Tung University and Ph.D. degree at the Institute of Computer Science, National Chung Hsing University, Taiwan. He is presently an associate professor of Department of Applied Mathematics, Nation Chiayi University. His research interests include information security and computer graphics.

Jyun-Ci Huang received his M.S. in Department of

Computer Science and Information Engineering from National Chiayi University in 2008. His research interests include information security, and image security.

Tzung-Her Chen was born in Tainan, Taiwan, Republic of China, in 1967. He received the B.S. degree in Department of Information & Computer Education from National Taiwan Normal University in 1991 and the M.S. degree in Department of Information Engineering from Feng Chia University in 2001. In 2005, he received his Ph.D. degree in Department of Computer Science from National Chung Hsing University. He has been with Department of Computer Science and Information Engineering at National Chiayi University as Professor since August 2011. His research interests include information hiding, multimedia security, digital rights management, network security. He is an honorary member of the Phi Tau Phi Scholastic Honor Society.