Multimed Tools Appl (2017) 76:9667–9679
DOI 10.1007/s11042-016-3573-1

A new buyer-seller watermarking protocol without multiple watermarks insertion

Jyun-Ci Huang[1] · **Fuh-Gwo Jeng**[2] · **Tzung-Her Chen**[1]

Received: 25 August 2015 / Revised: 20 March 2016 / Accepted: 3 May 2016 /
Published online: 14 May 2016

Abstract Watermarking protocols are designed for tracing illegal distributors when unauthorized copies are found. So far, most of the proposed schemes set up two or more watermarks embedded to a copy by the seller before it was sold. The main potential concerns of multiple watermarking are the image quality would be damaged and any earlier embedded watermarks would be destroyed as well. Thanks to visual cryptography which encodes the secret image into two shares, and recovers the secret by collecting these two shares. Therefore, a new buyer-seller watermarking protocol is proposed in this paper by applying the technique of visual cryptography to Lei et al.'s scheme so as to free from the disadvantages of multiple-watermarking insertion.

Keywords Watermarking protocol · Copyright protection · Digital watermarking · Visual cryptography

1 Introduction

In a digital information explosion age, people take advantages of convenience and rapidness because billions of digital contents, such as movies, music, texts and photos, are brought from networking deployment and progress. Ubiquitous networks bring us convenience and privilege in knowledge-sharing. Yet, they also make it easier to transport and consume digital contents illegally. Therefore, some solutions to deter illegal piracy problems should be done.

Unlike data hiding [15, 17, 18] or fragile watermarking [1, 13, 16], robust watermarking, a technique for the copyright protection of digital contents, is a good way to solve illegal piracy problems [4, 8, 9, 12, 14, 20, 21, 23]. An *identical* copyright signal is embedded into a

✉ Tzung-Her Chen
thchen@mail.ncyu.edu.tw

[1] Department of Computer Science and Information Engineering, National Chiayi University, Chiayi City 60004, Taiwan

[2] Department of Applied Mathematics, National Chiayi University, Chiayi City 60004, Taiwan

multimedia content and extracted out for proving the lawful ownership later on. Besides, watermarking protocols are designed to trace illegal distributors [2, 3, 5–7, 10, 14, 22, 24] at the same time. A *unique* watermark embedded into each sold copy can be used to track illegal customers when suspicious distributors are found. In buyer-seller watermarking protocols, a seller inserts a unique watermark, used for copy deterrence, into a copy of the content before selling to a buyer. In such a way, it is possible to trace illegal buyers when unauthorized copies are found.

Firstly, Qian and Nahrstedt proposed a copyright-protection protocol [14] for the owner–customer relationship. The drawback of their protocol was the seller could possess the exact protected copy even though it had been sold, which implied that the buyer could claim that the found unauthorized copy was distributed by the seller. Thus, Memon and Wong [10] proposed an asymmetric watermarking protocol scheme, in which they defined the buyer to be the only one, who had the right to possess the watermarked content. Subsequently, Horng and Chen [5] improved Memon and Wong's scheme by enabling anonymous transactions between buyers and sellers so as to protect the privacy of the buyers. Inspired by Memon and Wong's scheme, Cheung and Curreem [3] proposed a second-hand watermarking protocol; however, Chen et al. [2] pointed out their potential security weakness and then presented an improved version with the property of anonymity. Actually almost at the same time, Lei et al. [7] proposed a buyer-seller watermarking protocol in 2004 and also pointed out that Memon and Wong's scheme would be at risk for the unbinding problem. The problem says that when a seller gets a copy, and transplants the watermark of this copy to another more expensive, he then accuses the copy's owner of illegal piracy. Apart from this, the anonymous problem was taken into considerations in Lei et al.'s scheme; thus, each buyer was given an anonymous certificate during each transaction to achieve the property of anonymity. Later on, Zhang et al. [24] presented a secure buyer-seller watermarking protocol without a trusted third party (TTP). Wu-Pang [22] and Katzenbeisser et al. [6] respectively proposed their buyer-seller watermarking protocols by adopting symmetric ciphers instead, different from those by adopting homomorphic public key encryption to reduce the computational cost.

For a secure and efficient watermarking protocol, some problems should be highlighted and discussed first.

- Piracy tracing problems: If a pirated copy is found, the system is able to disclose the identity of the illegal buyer.
- Symmetry problems: The seller should not be aware of the watermarked copy which is uniquely linked to the buyer; otherwise, the judge cannot determine which the real identity of the distributor is, the buyer or the seller, if one illegal copy is found.
- Unbinding problems: A situation says that a seller finds a copy and transplants the embedded watermark of this copy to another more expensive content, and then he accuses the copy's buyer of piracy.
- Buyer privacy exposure problems: The identity of a buyer should not be disclosed during transactions unless he is committed to be an illegal distributor.
- Multiple watermark insertion problems: Watermarking is designed to protect images. However, multiple watermarking resulted in the quality degradation of the protected images. In fact, the degradation is directly proportioned to the times of watermark-embedding. Ideally, an image would be embedded once only. Multiple watermarking obviously causes the problem of watermark detection ambiguity, which means the latter

watermark may damage the former so that accurate detection of the original watermark is more difficult.

Unfortunately, all aforementioned schemes [2, 3, 5–7, 10, 22, 24] required the seller to embed at least two watermarks into a digital content. To avoid the unwanted affection in embedding/extraction operations, these schemes were forced to have more complex watermark-embedding approaches.

To have a secure and efficient watermarking protocol, we apply visual crytography [11] into Lei et al.'s protocol to form a new buyer-seller watermarking protocol. When the seller finds an unauthorized copy, he reconstructs the transaction watermark. Accordingly, the system identifies the malicious buyer and sends the related transaction records to the judge as proof that the buyer is guilty of illegal piracy. The proposed protocol, compared with the related ones, can easily solve the problem of multiple watermarking to diminish the two concerns of image quality distortion and the earlier embedded watermarks been destroyed.

The rest of this paper is organized as follows. The techniques of privacy homomorphism and visual cryptography are briefly introduced in the next section. In Section 3, the proposed protocol is described in details. And the further discussions are given in Section 4. The concluding remarks are done in Section 5.

2 Preliminaries

2.1 Privacy homomorphism

The property of privacy homomorphism is usually considered as an encryption tool on processing encrypted data. Let (a, b) be two secrets and $(E(a), E(b))$ be their respective encrypted items. The privacy homomorphism shows $E(a)\otimes E(b) \equiv E(a\otimes b)$, which means the result of operating two encrypted items is equivalent to that of operating two secrets first and then encrypting it later on. RSA [19], one of the well-known cryptosystems, satisfies the property of privacy homomorphism. With respect to the watermark-insertion operator, the privacy homomorphism function of RSA shows $E(a)E(b) \equiv (a^e)(b^e) \equiv (ab)^e \bmod n \equiv E(ab) \bmod n$, where $E(.)$ is the RSA encryption algorithm with the public encryption key e and the modulus n.

2.2 Visual cryptography

The t-out-of-n visual cryptography, saying (t, n), was first proposed by Naor and Shamir [11] in 1995. For a secret, it will be split into n shares. If t or more shares are collected and stacked, the original secret can be disclosed. For example, let (2,2) be the visual cryptography and six 2×2 subpixels ▚, ▞, ▙, ▛, ▟, ▜ be its codebook, shown in Table 1. Now, suppose the secret is a binary image and the generated shares will be photocopied onto transparencies. As usual, the outputs of visual white pixels are transparent. Thus, two shares are generated as follows. Every pixel in the secret image will be encoded into two 2×2 subpixels for Share_1 and Share_2 respectively. The rule is one of the subpixels from the codebook chosen for a share to display the white if the pixel is white; otherwise, to display the black if the pixel is black. When two shares/transparencies are stacked, it is obvious from Table 1 that the result for a white pixel in the secret image would be one of the codebook; that is, ▚, ▞, ▙, ▛, ▟, ▜. Contrarily, the result for a black pixel of the secret image goes to ■ identically. Briefly speaking, the stacked

Table 1 Shares generated by codebook of (2,2) visual cryptography

Secret image	White pixel						Black pixel					
Share$_1$(S_1)												
Share$_2$(S_2)												
Stacked subpixels												

subpixels for a black pixel of the secret image go to all black. Therefore, we can reconstruct the secret image visually by the rule that if the stacked results are all-black subpixels, the corresponding pixel of the secret image is recovered as *black*; otherwise, it would be *white*.

Take a binary logo image for example. The secret image shown in Fig. 1a is encoded into two visual secret shares, shown in Fig. 1b and c. When stacking the two shares, we can have

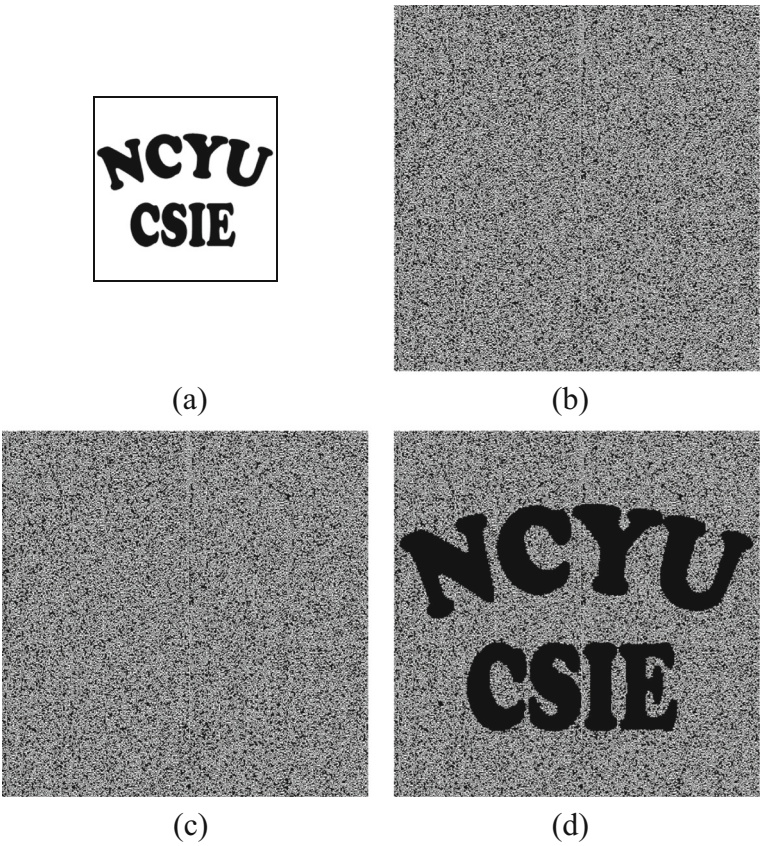


Fig. 1 **a** the secret image; **b**, **c** the corresponding (2,2) shares and **d** the stacked image

the reconstructed image, shown in Fig. 1d. To recognize the original secret image from the reconstructed one becomes easier.

3 The proposed scheme

To design a secure and efficient watermarking protocol, we apply the visual cryptography technique into Lei et al.'s protocol to form a new buyer-seller watermarking protocol so as to achieve the goal of diminishing the two main problems of multiple-watermarking insertion. Table 2 shows the notations used in this paper. It is worthwhile to note that any cryptosystem, not only RSA, satisfying the property of privacy homomorphism can be adopted.

3.1 Registration protocol

Suppose Buyer (***B***) with a pair of public keys (pk_B, sk_B) wants to keep anonymous during a transaction, he has to require an anonymous certificate from ***CA***. For ***B***, ***CA*** generates an anonymous certificate along with a short-term key pair (pk_B^*, sk_B^*) for the certain transaction. In the following is the registration protocol, depicted in Fig. 2.

1. ***B*** → ***CA***: *Cert*, pk_B.
   B sends ***CA*** his certificate (i.e. his identity) and his public key pk_B.
2. ***CA*** → ***B***: $Cert_{CA}(pk_B^*)$ and $E_{pk_B}(pk_B^*, sk_B^*)$.
   Once receiving pk_B, ***CA*** verifies the validation of the buyer. If true, he generates a pair of temporary keys (pk_B^*, sk_B^*) and an anonymous certificate $Cert_{CA}(pk_B^*)$ for ***B***. At the same time, ***CA*** encrypts the temporary keys as $E_{pk_B}(pk_B^*, sk_B^*)$ and then stores (pk_B, pk_B^*) in his database. Finally, he transmits $Cert_{CA}(pk_B^*)$ and $E_{pk_B}(pk_B^*, sk_B^*)$ to ***B***.
3 ***B*** decrypts $E_{pk_B}(pk_B^*, sk_B^*)$ first and then verify the validation of $Cert_{CA}(pk_B^*)$.

3.2 Watermarking protocol

Suppose ***B*** wants to purchase digital content X from seller (***S***), a common agreement between them, called *AGR*, has to be done first. Afterwards, *AGR* is regarded as a purchase contract

Table 2 The notations used in this paper

B, ***S***, ***CA***,***WCA***, ***J***: a buyer, seller, certification authority, watermark certification authority and the judge, respectively;

B → ***S***: *M*: participant ***B*** delivers message *M* to participant ***S***;

$E_k(.)$, $D_s(.)$: the encryption function with the public key k and decryption function with the private key s;

$Cert_I()$: the digital certificate issued by participant I.

$Sign_s(M)$: digital signature of message M signed by the private key s.

$S_A \leftarrow f_{VC}(O_V, S_B)$: the function $f_{VC}(,)$ with the inputs of a secret image O_V and a share image S_B outputs the other share image S_A, where $f_{VC}(.,.)$ is based on (2,2) *VC*.

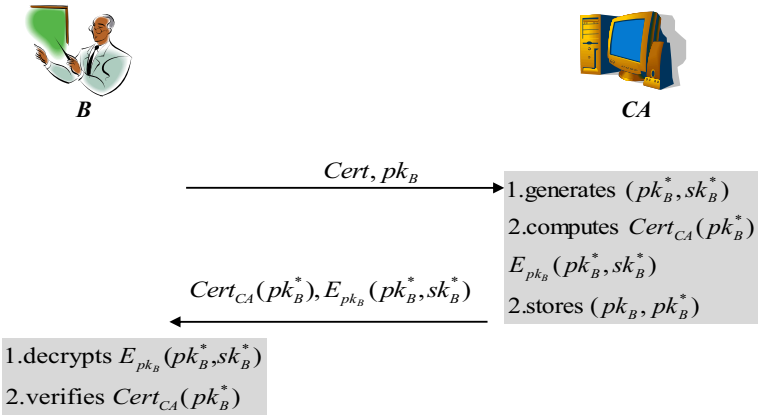


Fig. 2 Registration protocol

during this transaction, uniquely binding to digital content X. In the following is the watermarking protocol, depicted in Fig. 3.

1. ***B*** generates $Sign_{sk_B^*}(AGR)$ after he negotiates a common agreement, AGR, with ***S***.
2. ***B*** → ***S***: $Cert_{CA}(pk_B)$, AGR, $Sign_{sk_B^*}(AGR)$
3. When having these messages, ***S*** verifies whether $Cert_{CA}(pk_B^*)$ and $Sign_{sk_B^*}(AGR)$ valid or not. If yes, ***S*** generates a watermark O_V, which denotes the transaction information in a form of binary logo images.
4. ***S*** → ***WCA***: $Cert_{CA}(pk_B^*)$, AGR, $Sign_{sk_B^*}(AGR)$, O_V
5. When having these messages, ***WCA*** verifies whether $Cert_{CA}(pk_B^*)$ and $Sign_{sk_B^*}(AGR)$ valid or not. If yes, ***WCA*** generates a watermark S_W, randomly chosen from the VC codebook. Apart from watermark S_W, ***WCA*** also figures out the following messages, $E_{sk_{WCA}}(S_W)$, $E_{pk_B^*}(E_{sk_{WCA}}(S_W))$ and $S_1=Sign_{sk_{WCA}}\left(E_{pk_B^*}(E_{sk_{WCA}}(S_W))\ ||pk_B^*||Sign_{sk_B^*}(AGR)\right)$. Finally, he generates a secret share S_B by applying the visual cryptography function; that is, $S_B \leftarrow f_{VC}(O_C, S_W)$ and then calculates $E_{pk_S}(S_B)$. Note that if watermark S_W and secret share S_B are stacked, the watermark O_V is emerged from the stacked result.
6. ***WCA*** → ***S***: $E_{pk_B^*}(E_{sk_{WCA}}(S_W))$, s_1, $E_{pk_S}(S_B)$
7. When receiving these messages, ***S*** verifies s_1 first and decrypts $E_{pk_S}(S_B)$. And then he embeds $E_{pk_B^*}(E_{sk_{WCA}}(S_W))$ into X to have $E_{pk_B^*}(X')$, where $E_{pk_B^*}(X') = E_{pk_B^*}(X) \oplus E_{pk_B^*}(E_{sk_{WCA}}(S_W))$ and $\oplus$ is the operation of embedding. At last, ***S*** stores $E_{pk_B^*}(E_{sk_{WCA}}(S_W))$, $Cert_{CA}(pk_B^*)$, AGR, $Sign_{sk_B^*}(AGR)$, s_1, O_V, S_B into his database.
8. ***S***→***B***: $E_{pk_B^*}(X')$
9. ***B*** decrypts $E_{pk_B^*}(X')$ to get X', where $X'=X\oplus E_{sk_{WCA}}(S_W)$.

3.3 Identification and dispute protocol

Suppose ***S*** finds an unauthorized copy, called Y, he extracts $E_{sk_{WCA}}(S_W)$ from Y first and decrypts it to get S_W', where $S_W'=D_{pk_{WCA}}(E_{sk_{WCA}}(S_W))$. Then retrieving secret share



B ***S*** ***WCA***

1.generate s AGR, $Sign_{sk_B^*}(AGR)$

$Cert_{CA}(pk_B^*), AGR,$ $Sign_{sk_B^*}(AGR)$ →

1.verifies $Sign_{sk_B^*}(AGR)$ and $Cert_{CA}(pk_B^*)$
2.generates O_V

$Cert_{CA}(pk_B^*), AGR$ $O_V, Sign_{sk_B^*}(AGR)$ →

1.verifies $Sign_{sk_B^*}(AGR)$ and $Cert_{CA}(pk_B^*)$
2.generates $S_W, E_{sk_{WCA}}(S_W),$ $E_{pk_B^*}(E_{sk_{WCA}}(S_W)), s_1$
3. $f_{VC}(S_W, O_V) = S_B$
4. $E_{pk_S}(S_B)$

← $E_{pk_B^*}(E_{sk_{WCA}}(S_W))$ $s_1, E_{pk_S}(S_B)$

1.verifies s_1
2.decrypts $E_{pk_S}(S_B)$
3.embeds $E_{pk_B^*}(X') = E_{pk_B^*}(X) \oplus E_{pk_B^*}(E_{sk_{WCA}}(S_W))$

← $E_{pk_B^*}(X')$

1. $D_{sk_B^*}(E_{pk_B^*}(X'))$

Fig. 3 Watermarking protocol

S_i from each record of $\{E_{pk_B^*}(E_{sk_{WCA}}(S_W)), Cert_{CA}(pk_B^*), AGR, Sign_{sk_B^*}(AGR), s_1, O_V, S_B\}$ stored in his database, he stacks S_W' with share S_i to form a watermark saying O_{V_i}'. Then he compares O_{V_i}' and O_{V_i} with respect to S_i to decide the one with the highest correlation over the threshold of a predetermined confidence level. Note that this operation can be performed within a computation device. Finally, If O_{V_i}' and O_{V_i} are matched, the seller sends the corresponding whole record of the exact secret share S_i and the watermark O_{V_i} as well to J.

1. ***S*** →***J***: $E_{pk_B^*}(E_{sk_{WCA}}(S_W))$, $Cert_{CA}(pk_B^*)$, AGR, $Sign_{sk_B^*}(AGR)$, s_1, Y
2. ***J*** verifies whether $Cert_{CA}(pk_B^*)$, $Sign_{sk_B^*}(AGR)$ and s_1 valid or not. If yes, he computes $E_{pk_B^*}(Y)$ and checks whether $E_{pk_B^*}(Y)$ is a part of $E_{pk_B^*}(E_{sk_{WCA}}(S_W))$. If it is, ***J*** asks ***CA*** for the real identify of the buyer with pk_B^*.

Table 3 The comparison among the related schemes and the proposed scheme

Schemes	Memon and Wong [10]	Lei et al. [7]	Zhang et al. [24]	Wu and Pang [22]	Katzenbeisser et al. [6]	The proposed
Piracy tracing problem	No	No	No	No	No	No
Symmetry problem	No	No	No	No	No	No
Unbinding problem	Yes	No	No	No	No	No
Buyer privacy exposure problem	Yes	No	No	No	Yes	No
multiple watermarks insertion problem	Yes	Yes	Yes	Yes	Yes	No
WCA involved	Yes	Yes	No	Yes	Yes	Yes

4 Security analysis and discussions

In this section, we will demonstrate the security analysis and evaluate the performance of the proposed scheme. According to various security problems mentioned above, the comparisons are listed in Table 3. The performance comparisons of the proposed scheme and the related works in terms of computational cost are shown in Table 4.

Table 4 Comparison of performance among the related schemes and the proposed scheme for (a) registration and watermarking protocols and (b) Identification and dispute protocol

(a)

Operations	Embedding	Signing/verifying	Public-key en(de)cryption	Symmetric-key en(de)cryption
Schemes	*B*/*S* /*CA*/*WCA*/*J*	*B*/*S* /*CA*/*WCA*/*J*	*B*/*S* /*CA*/*WCA*/*J*	*B*/*S* /*CA*/*WCA*/*J*
Memon-Wong [10]	0 / 2 / 0 / 0 / 0	1 / 1 / 0 / 2 / 0	1 / 1 / 0 / 1 / 0	0 / 0 / 0 / 0 / 0
Lei et al. [7]	0 / 2 / 0 / 0 / 0	3 / 4 / 2 / 3 / 0	1 / 1 / 0 / 2 / 0	0 / 0 / 0 / 0 / 0
Zhang et al. [24]	0 / 2 / 0 / 0 / 0	3 / 3 / 2 / 0 / 0	2 / 2 / 0 / 0 / 0	0 / 0 / 0 / 0 / 0
Wu and Pang [22]	1 / 1 / 0 / 0 / 0	0 / 0 / 0 / 0 / 0	1 / 1/ 0 / 2 / 0	1 / 1 / 0 / 2 / 0
Katzenbeisser et al. [6]	1 / 0 / 0 / 0 / 0	1 / 1 / 0 / 1 / 0	1 / 0 / 0 / 1 / 0	1 / 1 / 0 / 3 / 0
The proposed	0 / 1 / 0 / 0 / 0	2 / 3 / 2 / 3 / 0	2 / 2 / 1 / 3 / 0	0 / 0 / 0 / 0 / 0

(b)

Operations	Extraction	Signing/verifying	Public-key en(de)cryption
Schemes	*B*/*S* /*CA*/*WCA*/*J*	*B*/*S* /*CA*/*WCA*/*J*	*B*/*S* /*CA*/*WCA*/*J*
Memon-Wong [10]	0 / 1 / 0 / 0 / 1	0 / 0 / 0 / 0 / 1	0 / 0 / 0 / 0 / 1
Lei et al. [7]	0 / 1 / 0 / 0 / 1	0 / 0 / 0 / 0 / 4	0 / 0 / 0 / 1 / 1
Zhang et al. [24]	0 / 1 / 0 / 0 / 1	0 / 0 / 0 / 0 / 3	1 / 0 / 0 / 0 / 0
Wu and Pang [22]	0 / 1 / 0 / 0 / 0	0 / 0 / 0 / 0 / 0	0 / 0 / 0 / 0 / 0
Katzenbeisser et al. [6]	0 / 1 / 0 / 0 / 1	0 / 0 / 0 / 0 / 2	0 / 0 / 0 / 2 / 0
The proposed	0 / 1 / 0 / 0 / 1	0 / 0 / 0 / 0 / 3	0 / 1 / 0 / 0 / 1

4.1 Security analysis

Five propositions will be presented to demonstrate that the proposed scheme can address the security problems highlighted above.

Proposition 1 *The proposed scheme can resist the piracy tracing problem.*

Proof.

In the identification and dispute protocol (Section 3.3), ***S*** can find the identity of the potentially malicious buyer ***B***. If ***B*** did illegally distribute copy *Y*, ***J*** would successfully assure that $E_{pk_B^*}(E_{sk_{WCA}}(S_W))$ did exist in $E_{pk_B^*}(Y)$ and asked ***CA*** for the real identity of the buyer with pk_B^*.

Proposition 2 The proposed scheme can resist the buyer privacy exposure problem.

Proof.

The proposed scheme takes the advantage of anonymous certificates to keep the anonymity of ***B***. ***B*** uses his anonymous certificate during transaction such that what ***S*** can track is the pseudonym. The pseudonym keeps ***B*** anonymous, unless he is confirmed to be guilty by ***J***. Without revealing the real identity of ***B***, ***B***'s privacy will not be compromised.

Proposition 3 The proposed scheme can resist the symmetry problem.

Proof.

Suppose ***S*** wants to cheat ***B***, he distributes a watermarked copy *X*', which has already been sold to ***B***. However, ***S*** does not know the identity of ***B*** (by **Proposition 2**) and he also has no idea which the exact copy is sold even if he has the list of the customers/members. Moreover, based upon the privacy homomorphism, the embedding is executed in the format of ciphers. ***S*** cannot decrypt the messages $E_{pk_B^*}(X')$, $E_{pk_B^*}(X)$ and $E_{pk_B^*}(E_{sk_{WCA}}(S_W))$ he holds without the corresponding short-term private key sk_B^*. Therefore, the only participant that can decrypt the encrypted copy $E_{pk_B^*}(X')$ is ***B***. Since ***S*** does not know the exact watermarked copy in the proposed protocol, ***B*** cannot claim that the unauthorized copy is resold or distributed by ***S***. The asymmetry property is proved.

Proposition 4 The proposed scheme can resist the unbinding problem.

Proof.

For the unbinding problem, the signature $s_1=Sign_{sk_{WCA}}\left(E_{pk_B^*}(E_{sk_{WCA}}(S_W))\ ||pk_B^*||Sign_{sk_B^*}(AGR)\right)$ binds S_W to *AGR* together with pk_B^*. It provides the proof that the buyer purchases content *X* binding with the transaction document *AGR*. Hence, ***S*** has no feasible way to transplant the watermark to the other contents.

Proposition 5 The proposed scheme can resist the multiple watermark insertion problems.

Proof.

Due to one and only one watermark S_W is embedded in the proposed protocol, it is trivial to show that our scheme has no problem with the multiple watermarking.

From the five propositions, the proposed scheme obviously can solve the problems when designing a secure and efficient watermarking protocol, especially the multiple-watermarking insertion problem. Table 3 depicts how well the proposed scheme works when compared with the related schemes, in terms of functionalities resisting the essential requirements such as piracy tracing problems, symmetry problems, unbinding problems, buyer privacy exposure problems, and multiple watermark insertion problems.

4.2 Computational cost

Table 4 shows the computation cost among the related works and the proposed scheme. Note that the computational cost of asymmetric cryptography is 100 to 1000 times of that of symmetric cryptography. Thus, the proposed scheme decreases the number of watermark embedding incidences without increasing computation cost significantly.

Claim 1 The proposed scheme is efficient other than security resistance.

Proof.

Comparing with the related works, the proposed scheme has no problem with the multiple-watermarking insertion. Clearly, the proposed scheme requires the time of watermark embedding only once. It then saves additional time because embedding a watermark needs extra complex computation of mathematic operations such as discrete cosine/wavelet transform over the whole image/audio/video. Moreover, by the technique of visual cryptography to trace the illegal distributor, the computation cost involving Boolean OR operation is trivial and can be neglected. The extra en(de)cryption or signature signing/verifying operations (referring to Table 4) are mainly introduced to solve the security problems existing in Ref. [7, 10, 24]. Thus the proposed scheme is efficient other than security resistance.

Claim 2 The proposed scheme is practical other than security resistance.

Proof.

The practicality of this scheme depends on the deployment cost of trusted third parties. In reality, the less memory the trusted third party needs for storing buyer's identity, public key, pseudonym, and so on, the less costly the system will be. In the proposed scheme, each trusted third party (***CA***, ***WCA***, and ***J***) can be of no memory devices. ***WCA*** and ***J*** are not required to maintain a database to store users' information. In the registration phase, ***CA*** stores ***B***'s public key and his pseudonym. However, ***CA*** can encrypt every pk_B and stores it in the extension field of each anonymous certificate $Cert_{CA}(pk_B^*)$. Therefore, it is unnecessary for ***CA*** to memorize the association between the real identities and the anonymous certificates. Since the proposed scheme can be designed to utilize low-cost trusted third parties, it is practical for purpose other than security resistance.

5 Concluding remarks

The conjunction of cryptosystems and watermarking schemes provides a feasible approach for piracy tracing. In this paper, we highlight the way of designing a general model for buyer-seller

watermarking protocol by introducing computation-cheap visual cryptography to reduce the possible damages of multiple watermarking.

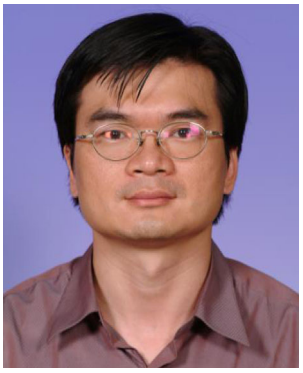
Acknowledgments This work was partially supported National Science Council, Taiwan, R.O.C., under contract by NSC 102-2221-E-415-014 and NSC 102-2221-E-415-007.

References

1. Chang CC, Chen YH, Kieu TD (2010) A watermarking technique using synonym substitution for integrity protection of XML documents. ICIC Express Lett 4(1):89–94
2. Chen TH, Horng G, Tsai D (2005) An anonymous buyer-reseller watermarking protocol. J Chin Inst Eng 28(3):535–538
3. Cheung SC, Currem H (2002) Rights protection for digital contents redistribution over the Internet. In: Proceedings of 26th Annual International Computer Software and Applications Conference, pp 105–110
4. Gu Q, Gao T (2009) A novel reversible watermarking algorithm based on wavelet lifting scheme. ICIC Express Lett 3(3 (A)):397–402
5. Horng G, Chen TH (2003) An anonymous buyer-seller watermarking protocol. Int J Comput Numer Anal Appl 4(4):423–432
6. Katzenbeisser S, Lemma A, Celik MU, Veen MVD, Maas M (2008) A buyer–seller watermarking protocol based on secure embedding. IEEE Trans Inf Forensics Secur 3(4):783–786
7. Lei CL, Yu PL, Tsai PL, Chan MH (2004) An efficient and anonymous buyer-seller watermarking protocol. IEEE Trans Image Process 13(12):1618–1626
8. Lin PL (2001) Digital watermarking models for resolving rightful ownership and authenticating legitimate customer. J Syst Softw 55(3):261–271
9. Lin PY (2014) Imperceptible visible watermarking based on postcamera histogram operation. J Syst Softw 95:194–208
10. Memon N, Wong PW (2001) A buyer-seller watermarking protocol. IEEE Trans Image Process 10(4):643–649
11. Naor M, Shamir A (1995) Visual cryptography. In: Proceedings of EUROCRYPT'94, LNCS, 950, pp 1–12
12. Pei SC, Guo JM, Lee H (2005) Novel robust watermarking technique dithering halftone images. IEEE Signal Process Lett 12(4):333–336
13. Qi X, Qi J (2007) A robust content-based digital image watermarking scheme. Signal Process 87(6):1264–1280
14. Qian L, Nahrstedt K (1998) Watermarking schemes and protocols for protecting rightful ownership and customer's rights. J Vis Commun Image Represent 9(3):194–210
15. Qin C, Chang CC, Huang YH, Liao LT (2013) An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism. IEEE Trans Circuits Syst Video Technol 23(7):1109–1118
16. Qin C, Chang CC, Chen PY (2012) Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism. Signal Process 92(4):1137–1150
17. Qin C, Chang CC, Chiu YP (2014) A novel joint data-hiding and compression scheme based on SMVQ and image inpainting. IEEE Trans Image Process 23(3):969–978
18. Qin C, Chang CC, Hsu TJ (2015) Reversible data hiding scheme based on exploiting modification direction with two steganographic images. Multimedia Tools Appl 74(15):5861–5872
19. Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2):120–126
20. Shieh JM, Lou DC, Chang MC (2006) A semi-blind digital watermarking scheme based on singular value decomposition. Comput Stand Interfaces 28(4):428–440
21. Subramanyam AV, Emmanue S, Kankanhalli MS (2012) Robust watermarking of compressed and encrypted JPEG2000 images. IEEE Trans Multimedia 14:703–716
22. Wu Y, Pang H (2008) A lightweight buyer-seller watermarking protocol. Adv Multimedia 2008:1–7
23. Yang CY, Hu WC, Hwang WY, Cheng YF (2010) A simple digital watermarking by the adaptive bit-labeling scheme. Int J Innov Comput Inf Control 6(3(B)):1401–1410
24. Zhang J, Kou W, Fan K (2006) Secure buyer-seller watermarking protocol. IEEE Proc Inf Secur 153(1):15–18

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.

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 associated professor of Department of Applied Mathematics, Nation Chiayi University. His research interests include information security and computer graphics.



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.