An Efficient Anonymous Buyer-Seller Watermarking Protocol

Chin-Laung Lei and Ming-Hwa Chan
,
Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan 106
Email: lei@cc.ee.ntu.edu.tw

Abstract

In order to deter unauthorized duplication and distribution of multimedia content, the seller can insert a unique watermark with respect to each buyer into a copy of the content. Then the seller can find out the original buyer of unauthorized copies using the corresponding watermark detection or extraction algorithm. However, the accused buyer can claim that the found unauthorized copies are created and distributed by the seller herself because the watermark is embedded solely by the seller. In this paper, a watermarking protocol is proposed to make the seller embed the watermark into a copy to be sold in encryption domain so that she cannot glean the watermarked copy exactly. This prevents the buyer from claiming that an unauthorized copy may have originated from the seller. In comparison with previous solutions, the proposed scheme is more convenient for buyers as they only have to interact with one party, the seller, each time they want to buy something. Besides, the proposed scheme enables buyers to buy multimedia content anonymously. However, upon finding an unauthorized copy at a later point in time, the seller can find the related record by detecting the embedded watermark in that copy and then provide this evidence to the judge to identify the cheating buyer in the trial.

Keywords: Copyright Protection, Watermarking, Privacy, Security

1. Introduction

The past few years have seen a rapid growth in the use of digital media. The contents of digital media are easy to duplicate and edit, and the distribution of them is becoming faster and easier as the computers are more and more integrated via Internet. However, these advantages also facilitate unauthorized copying and redistribution. The lack of effective intellectual property protection of digital media has become an important issue. Hence there has been an urgent need in developing multimedia copyright protection mechanisms.

Digital watermarking techniques have been introduced in recent years as methods to protect the copyright of multimedia data, and there has been various watermarking schemes applied to images and several methods applied to audio and

video streams. A watermark is a signal added to the digital data which can later be extracted or detected to make an assertion about the data [6]. In general, the watermark could be *visible* or *invisible*. A visible watermark typically contains a noticeably visible message or a company logo to indicate the rightful ownership of the content. On the other hand, invisible watermarks are unobtrusive modification to the content, and the invisibly watermarked content appears perceptually very similar to the original. The existence of an invisible watermark can only be determined by using a proper watermark extraction or detection algorithm. This kind of watermarks is generally preferred as their invisibility makes them more desirable.

This paper would focus on the applicability of invisible watermarking techniques for identifying the original distributor of a piracy copy. Consider the application where multimedia content is electronically distributed over a network. In order to discourage unauthorized duplication and distribution, the seller can insert a unique watermark (or a fingerprint), which could be used to trace unauthorized copies to the dishonest buyer, in each copy of the data that is to be sold. If, at a later point of time, an unauthorized copy of the data is found, the seller can determine the erring buyer by retrieving the unique watermark binding to each buyer in the unauthorized copy.

The major impediment, first represented as *customer's right problem* in [7], with traditional watermarking based fingerprinting techniques is that the seller exactly has the watermarked copy that the buyer obtained as the watermark is embedded by the seller. Thus, a buyer whose watermark has been found in unauthorized copies can argue that the unauthorized copy was originated by the seller. This could be done for example, by a malicious seller who may be interested in framing the buyer, or by a reselling agent who could potentially benefit from making unauthorized copies [7]. Even though the seller was not malicious, an unauthorized copy containing the unique watermark corresponding to the buyer could have originated from a security breach in the seller's system and not from the buyer.

In order to address this problem, Qian and Nahrstedt [7] propose an owner-customer watermarking protocol, but does not effectively solve the problem because the seller, in their scheme, still knows the exact copy in each buyer's possession, and the buyer can make the same claim, that an unauthorized copy was originated by the seller or by a security breach in the seller's system, as mentioned above. Memon and Wong [5] propose a buyer-seller watermarking protocol, which successfully solve customer's right problem. However, this scheme is inconvenient

for the public to use as the user has to interact with more than one party each time he wants to buy something. Besides, their scheme is not very flexible as the watermarking techniques applicable to this scheme are limited to be linear.

One important issue omitted by the previous schemes is to protect user privacy in the electronic world. Today, the computerized world has given us the ease of finding information we are looking for. At the same time it is increasingly difficult to keep personal information, which may be on line for some specific requirements, private. In addition, the maturity of data mining techniques enables the seller to learn a lot of information about a person's lifestyle, habits, etc., through what the buyer buys on line. Fortunately, in many cases such effects can be eliminated by applying appropriate cryptographic tools.

In this literature, a new protocol, which is more efficient, more flexible, and more convenient for the public to use than the previous solutions are, is proposed to address customer's right problem effectively. That is, the seller cannot know the watermark and the watermarked copy that the buyer obtains so she cannot create copies of the original content containing the buyer's watermark. Thus, a cheating buyer cannot make a claim as mentioned above when an unauthorized copy distributed by him has been found. In addition, the proposed protocol enables buyers to keep anonymous, but can nevertheless be identified if they distribute unauthorized copies.

The rest of this paper is organized as follows. Section 2 describes the proposed anonymous buyer-seller watermarking protocol in detail. It includes three subprotocols i.e., registration protocol, watermarking protocol, and identification and arbitration protocol. Section 3 examines how the proposed scheme fulfills its security requirements step by step and shows the improvements of the proposed scheme in comparison with previous solutions. Section 4 concludes the remarks about this paper.

2. The Proposed Scheme

We first introduce some notations and state certain assumptions followed by the detailed description of the proposed protocol. In this paper, S is the seller, who may be the original content owner or a reselling agent. B is the buyer, who would like to buy the copy or copies of some digital content from the seller. It is assumed

at the start of the proposed scheme, each party, such as the seller, the buyer, and all of the third parties, already possesses a key pair (sk, pk) of a digital signature scheme, and all of which have been registered with appropriate certification authorities; so that the public key can serve as a digital identity, and we do not have to fix how the validity of the initial digital identity is verified. Thus we can request any party, such as the buyer, to sign something under his identity in the protocol. $Sign_I(M)$ represents that the message M is signed under the identity I. More precisely, that means M is signed by I's private key sk_I, and it should be verified using I's corresponding public key pk_I.

Each buyer also has to register specifically for the proposed scheme under his digital identity. After finishing registration, the buyer will be assured to be anonymous among the users of the registration center with which he registered. The parties where registration can be done are called registration centers, simply represented as RCs. There can be one or more available registration centers in the proposed scheme at the same time, and more than one organization are appropriate to offer the registration service. For example, it can be the certification authority that issues the certificate of the key pair each party possesses. Another reasonable candidate for RC is the buyer's bank because, in order to offer integrated anonymity, the buyer has to register with a bank to pay for the watermarked copy with anonymous electronic cash. The registration centers will not disclose the registration records of buyers to anybody, except that the arbiter shows some buyer who should be responsible for a redistributed copy and then asks the registration centers for the corresponding record.

For ease of illustration, we assume that the content being sold is a still image, although in general the proposed scheme is also applicable to audio and video data. We use X to represent an original image and W as the watermark that will be inserted into X. Any watermarking technique that is an invisible and robust scheme is appropriate to the proposed protocol. The watermark insertion step of the adopted watermarking technique can be represented as

$$X' = X \oplus W \tag{1}$$

where X' is the watermarked image and $\oplus$ is the insertion operation.

We assume the existence of a public key cryptosystem that is a *privacy homomorphism* with respect to the binary operator $\oplus$. By privacy homomorphism

with respect to $\oplus$ it means the public key cryptosystem has the property that

$$E_K(a \oplus b) = E_K(a) \oplus E_K(b) \quad (2)$$

for every a and b in the message space. Here $E_K(\cdot)$ is the encryption function and K is the public key. For example, the well-known RSA public key cryptosystem [8] is a privacy homomorphism with respect to multiplication [9]. Another public key encryption function that is a privacy homomorphism with respect to addition is given in [2].

In order to construct a real anonymous framework, anonymous communication and anonymity controlled electronic payment systems are necessary. Anonymous communication makes the receiver unable to determine from which IP address the message originates, and anonymity controlled payment systems allow buyers to pay for things anonymously in order to offer similar privacy as with physical cash. Equipped both of them, the framework ensures that it is unlikely to leak any information about the buyer's true identity. Most of the previous anonymity related research can be slightly modified to fit in the proposed scheme; so we just assume the existence of the suitable anonymous communication technique and anonymous cash-like payment system and then focus on the proposed scheme itself.

Besides, we also assume there is a trusted watermark certification authority, simply represented as WCA, who randomly generates watermarks in the required manner and issues them to the seller upon request. The watermark certification authority is memoryless here and does not maliciously reveal or keep track of the issued watermarks. Finally, we assume there is a trusted arbiter, simply represented as A, who should be convinced in trials. After accepting to deal with the accusation made by the seller, the arbiter will retrieve the real identity of a suspect and justly judge whether the identified buyer is guilty or not according to the collected evidence.

The anonymous buyer-seller watermarking protocol that we will present in this section consists of three subprotocols: registration protocol, watermarking protocol, and identification and arbitration protocol. They are deliberated respectively in the following.

A. Registration Protocol

In registration, the buyer selects a key pair (sk^*, pk^*) of the chosen public key

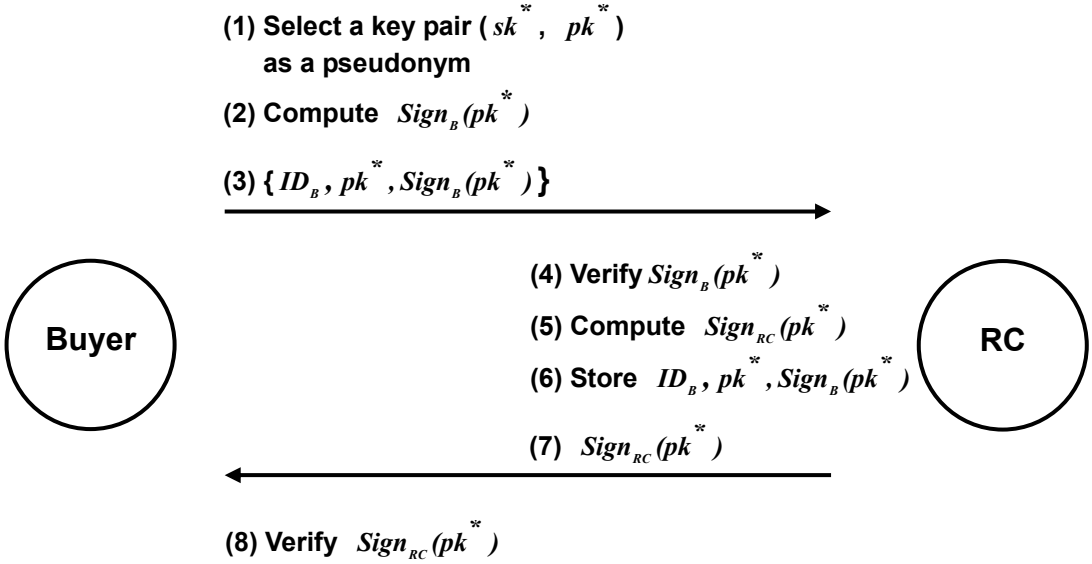

Figure 1. Registration Protocol

cryptosystem that is a homomorphism with respect to the watermark insertion operation $\oplus$, sk^* is the private key and pk^* is the public key, and signs pk^* under his normal identity that he will be responsible for this pseudonym. Using pseudonyms to allow users to interact with multiple organizations anonymously were first introduced by Chaum [1] in 1995. The pseudonyms cannot be linked but are formed in such a way that a user can prove to one organization a statement about his relationship with another. After establishing his pseudonym and the signature of the pseudonym under his real identity, the buyer sends both pk^* and $Sign_B(pk^*)$ along with his identity ID_B to the registration center RC. Upon receiving this information, the registration center first verifies $Sign_B(pk^*)$. If the signature is incorrect, this protocol fails; or the registration center saves pk^*, $Sign_B(pk^*)$, and ID_B in its database and then sends to the buyer the signature $Sign_{RC}(pk^*)$, that certifies the validity of the pseudonym. Finally, the buyer is able to form a certificate $(pk^*, Sign_{RC}(pk^*))$, which shows that the registration center guarantees the authenticity of such information that it provides. More intuitively, this certificate means that the registration center declares that it knows the real identity of the buyer who uses this pseudonym.

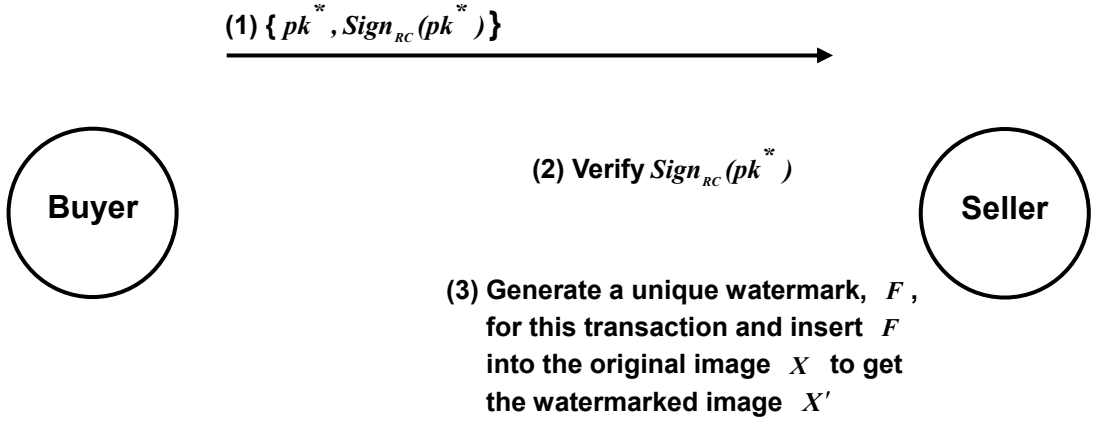

Figure 2. Watermarking Protocol (I)

B. Watermarking Protocol

When the buyer wants to buy an image from the seller, he sends the seller his pseudonym pk^* along with the signature $Sign_{RC}(pk^*)$ of the registration center RC. The seller first verifies $Sign_{RC}(pk^*)$ in order to make sure that pk^* is indeed a valid pseudonym certified by the registration center RC.

,Let X denote the original image that the buyer wants to purchase from the seller. The seller generates a unique watermark, F, for this transaction, and then she embeds F into the image X to obtain the watermarked image X'. Note that in this step, the seller is free to use any suitable watermarking scheme of her choosing, public or private, spatial domain or transform domain, linear or nonlinear. "Suitable" means the chosen watermarking scheme should be robust in order to counter post image processing or malicious attacks that are possibly encountered later. The watermark F is not the watermark the seller will use to prove that the buyer has made illegal copies of an image. The primary purpose of F is to enable the seller to identify an illegal copy and search the recorded entry with respect to that copy in her database.

The seller then sends the buyer's pseudonym pk^* and $Sign_{RC}(pk^*)$ to the watermark certification authority WCA and requests a valid watermark. The watermark certification authority, after verifying $Sign_{RC}(pk^*)$, randomly generates a watermark W in the required manner and sends back to the seller $E_{pk^*}(W)$, the watermark encrypted with pk^*, along with a digital signature $Sign_{WCA}(E_{pk^*}(W))$

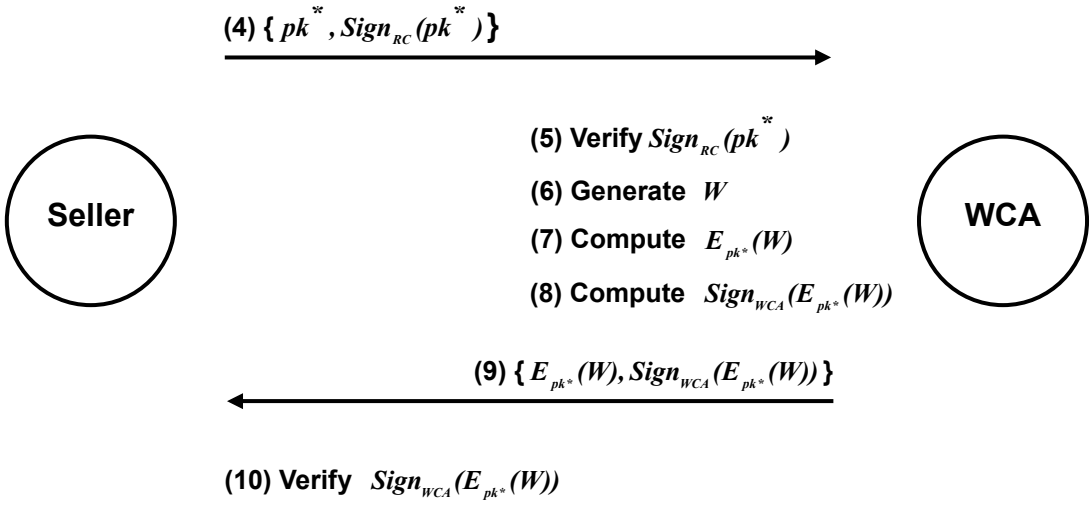

Figure 3. Watermarking Protocol (II)

that certifies the validity of the encrypted watermark.

After verifying $Sign_{WCA}(E_{pk*}(W))$, the seller inserts the encrypted watermark obtained above as a second watermark into the already watermarked image X'. Since the watermark received from the watermark certification authority is encrypted with the public key pk^* of the buyer's pseudonym, the seller embeds this second watermark in the encrypted domain also using pk^* which is already known to her. Inserting a watermark in the encrypted domain is feasible because the public key cryptosystem being used is a homomorphism with respect to $\oplus$, the insertion operation of the watermarking technique used in this scheme. That means, the seller computes

$$\begin{aligned} E_{pk*}(X'') &= E_{pk*}(X') \oplus E_{pk*}(W) \\ &= E_{pk*}(X' \oplus W) \quad . \end{aligned} \tag{3}$$

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

The seller has to store pk^*, $Sign_{RC}(pk^*)$, $E_{pk*}(W)$, $Sign_{WCA}(E_{pk*}(W))$, and F in $Table_X$. $Table_X$ is a table of records maintained by the seller for image X and contains one entry for each sold copy of the image X. Each entry in this table contains the public key pk^* of the buyer's pseudonym along with the signature $Sign_{RC}(pk^*)$ of the registration center, the encrypted watermark $E_{pk*}(W)$ that she received from the watermark certification authority along with its signature

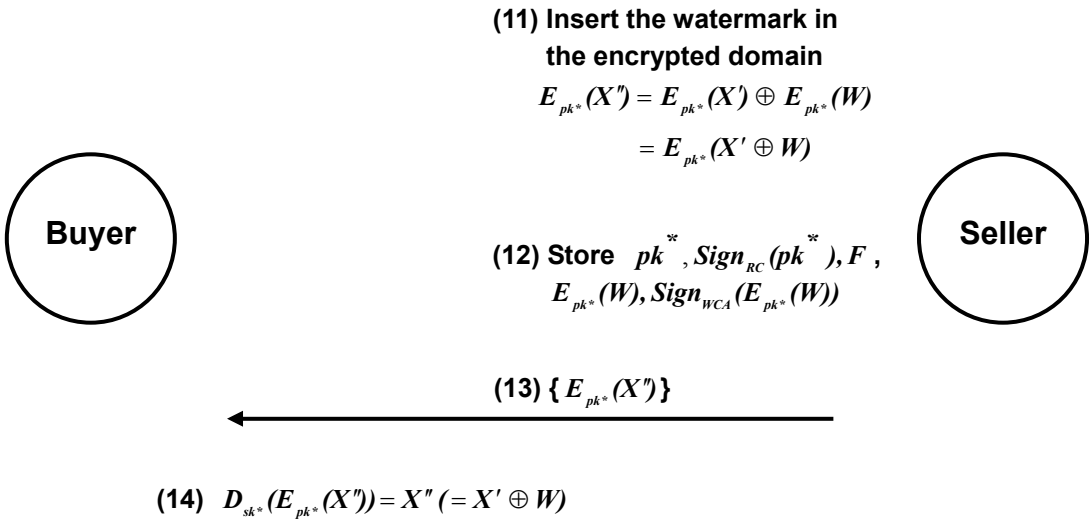

Figure 4. Watermarking Protocol (III)

$Sign_{WCA}(E_{pk*}(W))$ proving the validity of the watermark, and finally the unique watermark F known only to her that corresponds to a particular purchase.

After receiving the encrypted watermarked copy, the buyer just decrypts the data from the seller to obtain a watermarked image X''. That is to say the buyer computes

$$D_{sk*}(E_{pk*}(X'')) = X'' = X' \oplus W \tag{4}$$

where sk^* is the private key corresponding to the public key pk^*, and $D(\cdot)$ is the decryption function. Now the buyer has a watermarked copy X'' of X that the seller cannot reproduce because she does not know the embedded watermark W and the private key sk^*. Also, since the buyer does not know W it is more difficult for him to remove W from X''. Neither can he remove F which is also unknown to him.

C. Identification and Arbitration Protocol

When discovering an unauthorized copy, represented as Y, of the original image X, the seller can find out the purchase record with respect to this redistributed copy from $Table_X$ by detecting the unique watermark that she inserted for each transaction. This is done by running the corresponding watermark extraction or detection algorithm, which takes Y, and X if the watermarking technique used is a private

scheme, as input. Let G denote the watermark that is returned by the watermark extraction function. Using this extracted watermark G the seller then locates the purchase record with respect to Y in $Table_X$. The exact mechanism for locating the corresponding purchase record in $Table_X$ solely depends on the chosen watermarking technique. For example, if the watermark is robust, this would generally be accomplished by correlating G with every watermark F in $Table_X$ and selecting the one with the highest correlation beyond a confidence threshold. Once this F is located in $Table_X$, the seller reads the data kept in the located entry in $Table_X$, shows them along with Y to the arbiter, and then enters the identification and arbitration protocol. If G cannot be matched to any watermark F in $Table_X$ then the protocol returns failure.

After the seller sends the data located in $Table_X$, including pk^*, $Sign_{RC}(pk^*)$, $E_{pk*}(W)$, $Sign_{WCA}(E_{pk*}(W))$, and F, and the unauthorized copy Y to the arbiter, the arbiter first verifies $Sign_{RC}(pk^*)$ and $Sign_{WCA}(E_{pk*}(W))$ then, if both of the signatures are correct, requests the registration center RC to reveal the user identity with respect to pk^* in its stored registration records. The registration center returns to the arbiter the corresponding buyer's identity ID_B along with the signature $Sign_B(pk^*)$ as the evidence that proves the buyer should be responsible for this pseudonym. Now having known who the suspect buyer really is, the arbiter would send $E_{pk*}(W)$ to the buyer and ask him to decrypt it then return the result, W, back. The arbiter could then verify W by encrypting it with the corresponding public key pk^* and checking if the result equals to $E_{pk*}(W)$.

After verifying W, the arbiter can then run the watermark extraction or detection algorithm on Y and check if W is indeed present in Y. If the watermark W is indeed found in Y, the buyer is guilty otherwise the buyer is innocent. If the buyer is proved innocent in the trial, the arbiter will not show the seller the real identity of the buyer so that the buyer will still remain anonymous to the seller. Note that in the arbitration procedure the buyer has to take part in the protocol by decrypting $E_{pk*}(W)$ and then returning W back to the arbiter. If the buyer refuses to participate then this would be taken as an admission of guilt on the part of

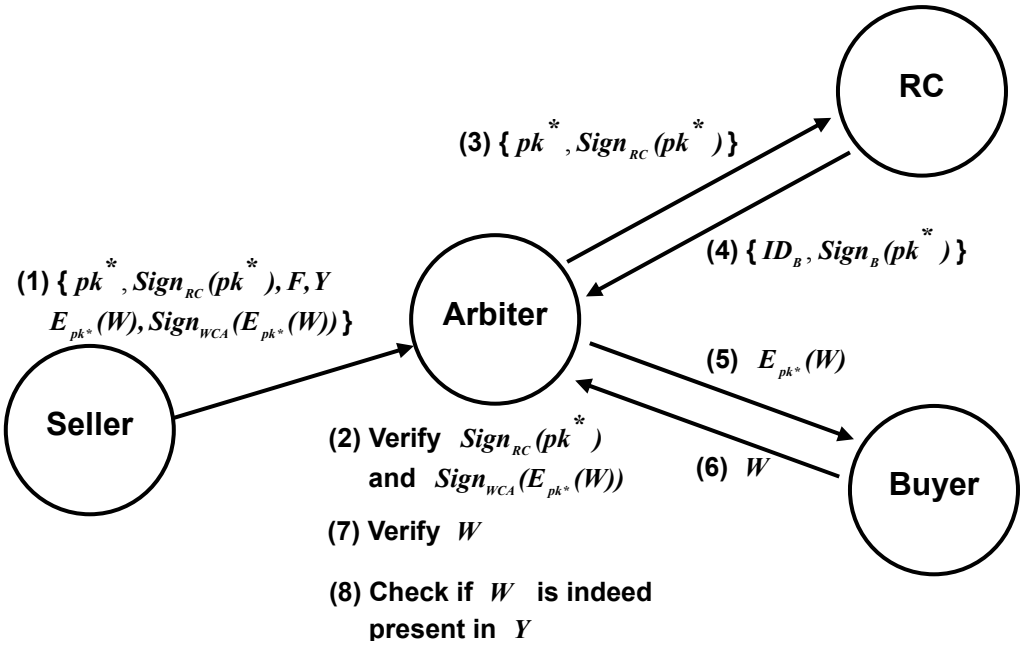

Figure 5. Identification and Arbitration Protocol

the buyer.

3. Discussion

The security of the proposed anonymous buyer-seller watermarking protocol is to be investigated in this section. The proposed scheme should assure that not only the buyer but also the seller to be protected from cheating behavior. We first indicate three requirements that should be fulfilled in the proposed scheme, and then, keeping the mentioned requirements in mind, further examine each of the three subprotocols respectively. Besides fulfilling the security requirements, the proposed scheme is more efficient, more flexible, and more convenient to buyers in comparison with the previous solutions. A modification for preventing the watermark to be exposed in the identification and arbitration protocol is also presented.

A. Requirements

1) Effectiveness

The proposed scheme should be effective in the sense that all of the subprotocols end successfully, and the buyer should obtain a useful copy of the image that he wants to buy if all parties are honest within the protocol execution. “Useful” means that

the embedded watermark does not affect the perceptual quality of the watermarked copy obtained by the buyer.

2) Security

The security of the proposed scheme should be considered in two aspects. First, the seller wants to be protected from deceitful buyers. If an illegal copy turns up, it is assured that a certain buyer will be identified and found guilty as responsible for that copy. More precisely, it should be infeasible for any deceitful buyer to find some way to remove or destroy the embedded watermark; so the seller is surely able to obtain a valid watermark with a proof to enter arbitration procedure when a redistributed copy is found and then wins a trial with any honest arbiter. Furthermore, as the seller's reputation will usually be damaged when accusing a buyer and then losing the trial, she should also be protected from making wrong accusations. So we require that there is no way for the cheating buyer to alter or fabricate a copy from which the seller identify someone successfully, but later the wrongly identified buyer is proved innocent in the trial.

Secondly, the buyer wants to be protected from a cheating seller and other erring buyers. If a buyer honestly takes part in the subprotocols and keeps the bought watermarked copy secret, he should not be falsely regarded as guilty by any honest arbiter no matter what the other parties act.

3) Anonymity

The buyer's real identity cannot be determined, and nothing about the purchase behavior or habits of the buyer becomes known to any other party if he acts honestly, except, if the registration center colludes.

B. Examination of Subprotocols

1) Registration Protocol

In the proposed scheme, the buyer has to register his pseudonym with the registration center RC first. If the digital signature scheme built in the beginning is secure, the buyer cannot fabricate an unregistered pseudonym as valid. After finishing the registration protocol, the buyer is able to buy digital images anonymously, and the seller cannot identify his real identity. However, all of his purchase record still can be linked to a pseudo-identity i.e., his pseudonym and then

can be gathered, accumulated, and analyzed for some attempts. One way to reduce such linkability is that the buyer can run this protocol several times in advance to prepare a set of valid pseudonyms and then randomly pick one of them to buy things anonymously. How many pseudonyms the buyer should register mainly depends on the degree of anonymity that the buyer prefers to maintain. Another way is that the buyer can stop using the pseudonym which has been used for a while and register again to exploit a new valid pseudonym. Again, how frequently the buyer should re-register and change to a new pseudonym depends on the degree of anonymity preferred.

2) Watermarking Protocol

Here, the seller requests and obtains an encrypted watermark and the corresponding digital signature of the encrypted watermark from the watermark certification authority WCA. If the encryption function and the digital signature scheme being used are secure, there is no way the seller could change or substitute the watermark by herself. For example, a malicious seller who attempts to frame the buyer could use pk^* to encrypt a watermark $\hat{W}$ generated by her own, then embed it into X' in the encrypted domain, and send this watermarked copy to the buyer. Although the seller, in this case, can duplicate and redistribute the watermarked copy in the buyer's possession, she cannot generate the signature $Sign_{WCA}(E_{pk*}(\hat{W}))$ which can prove the validity of the watermark. Hence the seller will lose the trial as she cannot offer sufficient evidence to convince the arbiter that she acts honestly but the buyer does not in identification and arbitration subprotocol.

After obtaining the encrypted watermark $E_{pk*}(W)$, the seller first inserts a watermark F, which she can later use to determine the source of an illegal copy, to get a watermarked copy X'. Obviously, it is against her own interest not to perform this step in the proper manner, as she will not be able to identify the corresponding purchase record with respect to an unauthorized copy. In the next step, she encrypts X' using pk^* and then inserts W into X' in the encryption domain. Again, it is against her interest not to perform this step in the required manner. For example, the seller could use a watermark obtained from the prior transaction with another buyer. In this case, when the buyer decrypts the encrypted watermarked image, he

would obtain a copy with severely degraded quality because the watermark and the image have been encrypted by different public keys. The seller could also use a watermark obtained from the same buyer before. Actually, no harm is done in this case because the buyer still can obtain a useful watermarked copy, and the seller still can convince the arbiter in the trial if a corresponding redistributed copy is found. The only problem is that the same watermark is used in two or more transactions. This can be prevented by inclusion of a time stamp, the information about the transaction, and their signatures of the watermark certification authority to ensure that the seller does properly follow what she supposed to do in the protocol.

If the encryption scheme of the public key cryptosystem being used is secure, the seller has no way of gleaning any information about the watermark W, and she cannot obtain or reproduce the watermarked copy by herself, either. Hence the buyer will not be framed by a dishonest seller. Meanwhile, if the underlying watermarking technique is secure and robust enough, it is infeasible for a cheating buyer to remove or destroy the embedded watermark without getting the image corrupted.

3) Identification and Arbitration Protocol

The seller first runs the watermark extraction or detection algorithm of the chosen watermarking technique and tries to use the result to find out the purchase record to which an unauthorized copy corresponds. At this point it is possible for the seller to mistakenly find another watermark inserted into the copy of another buyer. That is a false positive, which is highly undesirable. However, the different watermarks inserted into different copies of the content are uncorrelated because they are randomly generated by the watermark certification authority. As the seller has no knowledge about the watermark inserted into each copy and has seen it only in the encrypted form, it is highly unlikely that the seller would detect a false positive in the relatively small number of instances which she has at her disposal to try. Conclusively, in order to protect the seller from making wrong accusations, it is necessary using a watermarking technique with an acceptable false positive rate within the proposed scheme. Recent modes for predicting the false positive rate of a watermarking technique can be found in [3] and [4].

After retrieving the purchase record with respect to an unauthorized copy, the seller sends them along with that illegal copy as evidence to the arbiter. As mentioned above, when the underlying digital signature scheme and the encryption

function are secure, the seller is not able to fabricate this evidence. The registration center will keep the registration records safely and not reveal them except that the arbiter has verified the evidence and requests for the corresponding. This ensures that the buyer remains anonymous unless he illegally duplicates the watermarked copy in his possession and then distributes it. After receiving the response of the registration center, the arbiter now knows the suspect buyer's real identity with respect to the pseudonym pk^* and also obtains the signature $Sign_B(pk^*)$ as evidence that can prove the buyer should hold responsibility for this pseudonym.

The arbiter then requests the buyer to decrypt $E_{pk*}(W)$ and return the decrypted result. At this point, the cheating buyer can send some random watermark T instead. However, the seller has presented the arbiter with the encrypted watermark, $E_{pk*}(W)$, and this would not match with $E_{pk*}(T)$. Meanwhile, the buyer may refuse to cooperate with the arbiter, but as mentioned in the previous chapter this would be considered as an admission of guilt.

According to the discussion above, the security of the proposed anonymous buyer-seller watermarking protocol relies critically on the security of the underlying watermarking and encryption techniques used in the practical implementations. For example, if we use a watermarking technique whose insertion operation is multiplication and the RSA cryptosystem, which is an appropriate corresponding privacy homomorphism, the security of the proposed protocol just depends on both the security of the RSA cryptosystem and the chosen watermarking technique. Here, the RSA cryptosystem is a mature and well-studied technique that is believed secure if properly used [9]; so the proposed scheme, in this case, will be secure only as much as the chosen watermarking technique is secure and robust.

Note that the proposed protocol does not critically make use of the properties of any particular watermarking technique. As long as the watermarking technique is an invisible and robust scheme, it can be used in conjunction with a suitable public key cryptosystem that is a privacy homomorphism with respect to the insertion operation of the watermarking technique. Hence, if a better watermarking technique is developed later, it could be used in the proposed protocol.

C. Comparison with Previous Solutions

In general, a new proposed scheme will be adopted by the public users only

when it is easy to use. In the protocol proposed by Memon and Wong [5], every time the buyer intends to buy an image, he has to request a valid watermark from the watermark certification authority first and then is able to start the transaction with the seller. The necessity for the buyer to contact with more than one party during the purchase is inconvenient and probably unacceptable to the public users. On the other hand, the buyer in the proposed scheme can interact only with the seller to buy many images and be anonymous after registering at the beginning; so the proposed scheme is more convenient and acceptable to the public users.

Additionally, in the design of Memon and Wong [5], the buyer first obtains the watermark to be inserted from the watermark certification authority. In order to reduce the buyer's understanding of this specific watermark and to enhance the security of the applied watermarking technique, the seller has to generate a random permutation to scramble the elements of the encrypted watermark received from the buyer and store the result for future use in the arbitration procedure. However, only the linear watermarking techniques, in which both the watermark and the image can be represented as vectors, enable the seller to do the random permutation described above. This not only increases the seller's computation overhead but also reduces the flexibility of Memon and Wong's protocol. In our proposed scheme, on the contrary, the watermark is requested by the seller. The buyer does not have any information about the watermark so the seller does not have to do any additional processing on the encrypted watermark that she obtains before the watermark is inserted into the original image. This not only prevents that the buyer has auxiliary information to enable him to successfully attack the embedded watermark but also reduces the computation and storage requirements of the seller. The watermarking techniques, furthermore, no longer have to be limited as linear. As long as a watermarking technique is invisible and robust, it can be used in our proposed protocol. This makes our scheme more flexible.

D. Keep the Watermark Secret

In identification and arbitration protocols of the proposed scheme, the arbiter sends the encrypted watermark $E_{pk^*}(W)$ to the buyer and requests the buyer to decrypt it. At this point, the buyer learns W by decrypting $E_{pk^*}(W)$. This provides a dishonest buyer with the auxiliary information he needs to remove the

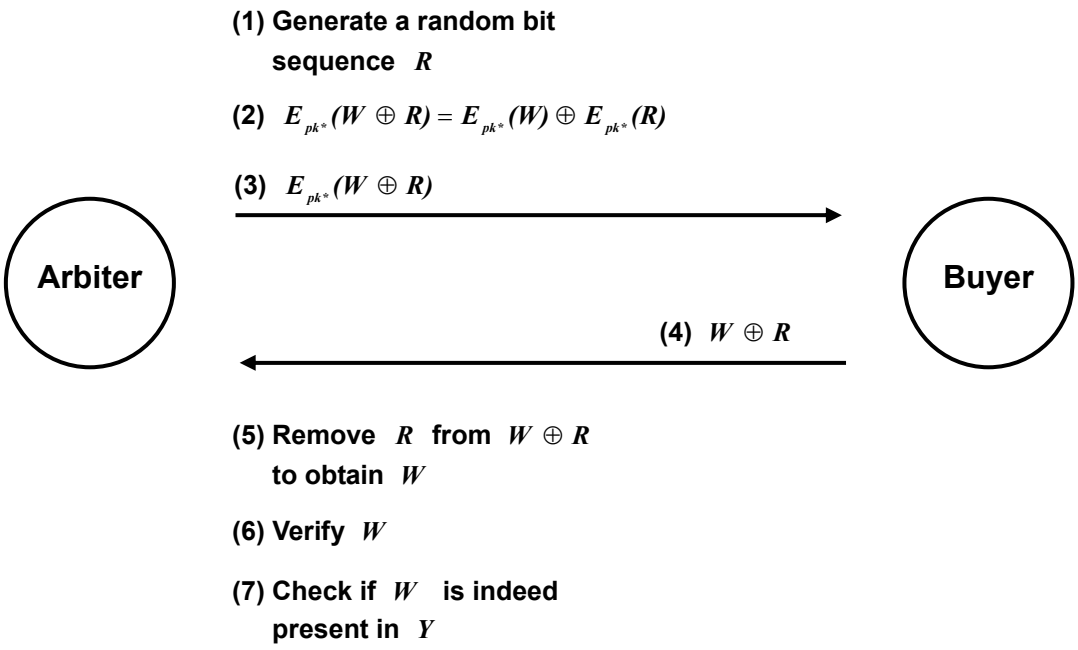

Figure 6. Keep the Watermark Secret to the Buyer

watermark. Here, we apply homomorphism property of the public key cryptosystem being used in the proposed scheme again and propose a solution which enables the arbiter to obtain the watermark W and keep it secret to the buyer at the same time

Before the arbiter sends the encrypted watermark $E_{pk*}(W)$ to the buyer, it randomly generates a bit sequence R first. Then it encrypts R by using the public key pk^* received from the seller and runs the binary operation $\oplus$, which may usually be addition or multiplication, on W and R in the encrypted domain. That is, the arbiter computes

$$E_{pk*}(W \oplus R) = E_{pk*}(W) \oplus E_{pk*}(R). \quad (5)$$

After the computation, the arbiter sends $E_{pk*}(W \oplus R)$ to the buyer and asks the buyer to decrypt it then return the result i.e., $W \oplus R$. Because the bit sequence R is randomly generated by the arbiter, the buyer cannot know R so that he cannot remove it from $W \oplus R$ to obtain W. Then the buyer sends the result, $W \oplus R$, back to the arbiter. After receiving $W \oplus R$, the arbiter is able to obtain W by removing R from $W \oplus R$ according to its knowledge about R. Finally, the arbiter run the corresponding watermark extraction algorithm on the illegal copy and checks if W is indeed present in that copy.

4. Conclusions

In this paper, an anonymous buyer-seller watermarking protocol is proposed to fulfill the requirements of copy deterrence and privacy protection at the same time. Although it seems that the goals of letting buyers purchase digital content anonymously and embedding a unique watermark with respect to each buyer for copy deterrence conflict to each other, the proposed scheme successfully resolves this seemingly conflict and achieves both goals. Besides, we discuss three problems that could happen in the present environment and provide corresponding solutions by modifying the proposed scheme. These discussions include how to solve key lost problem, how to keep the watermark secret while asking the buyer to decrypt the encrypted watermark, and how to use a proxy to offer anonymous communication on Internet today. In summary, the proposed scheme equips the following advantages. First, it is effective, i.e., it solves customer's right problem effectively. In the proposed scheme, the seller cannot know the exact watermarked copy that the buyer obtains as the watermark is embedded in the encryption domain. Hence the buyer cannot claim that an unauthorized copy found related to him may have originated from the seller because the seller cannot create copies containing the buyer's watermark. Second, the proposed scheme enables buyers to buy information anonymously. However, a dishonest buyer who illegally redistributes the copy he bought will be identified by the arbiter in the trial. Third, the proposed scheme is more convenient for buyers in comparison with the previous solution. After registering for his pseudonym, the buyer only has to interact with one party, the seller, to buy things rather than with the watermark certification authority first and then with the seller in [5]. Fourth, it is more efficient. In the proposed scheme, the seller does not have to generate a random permutation to scramble the encrypted watermark anymore as she does in [5]. This reduces its computation overhead and storage requirement. Last but not least, the proposed scheme is flexible as it can be used with any watermarking technique, as long as it is invisible and robust, and appropriate public key cryptosystems.

References

[1] D. Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete," *Communications of the ACM*, Vol. 28, No. 10, pp. 1030-1044, 1985.

[2] J. D. Cohen and M. J. Fischer, "A Robust and Verifiable Cryptographically Secure Election Scheme," in *Proceedings of IEEE 26th Symposium Foundations of Computer Science (FOCS'85)*, pp.372-382, October 1985.

[3] G. F. G. Depovere, A. C. C. Kalker, and J. P. M. G. Linnartz, "Improved Watermark Detection Reliability Using Filtering before Correlation," in *Proceedings of IEEE International Conference on Image Processing (ICIP'98)*, , pp. 430-434. October 1998.

[4] J. R. Hernández, F. Pérez-González, J. M. Rodriguez, and G. Nieto, "Performance Analysis of a 2-D-Multipulse Amplitude Modulation Scheme for Data Hiding and Watermarking of Still Images," *IEEE Journal on Selected Areas in Communications,* Vol. 16, No. 4, pp. 510-523, May 1998.

[5] 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.

[6] N. Memon and P. W. Wong, "Protecting Digital Media Content," *Communications of the ACM*, Vol. 41, No. 7, pp. 35-43, July 1998.

[7] L. Qiao 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, September 1998.

[8] R. Rivest, A. Shamir, and L. Adelman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126, 1978.

[9] D. Stinson, *Cryptography: Theory and Practice*. Chapman & Hall, 1995.