8-2008

# A Lightweight Buyer-Seller Watermarking Protocol

Yongdong WU
*Institute for Infocomm Research, Singapore*

Hwee Hwa PANG
*Singapore Management University*, hhpang@smu.edu.sg

**DOI:** https://doi.org/10.1155/2008/905065

Hindawi Publishing Corporation
Advances in Multimedia
Volume 2008, Article ID 905065, 7 pages
doi:10.1155/2008/905065

*Research Article*

# A Lightweight Buyer-Seller Watermarking Protocol

**Yongdong Wu[1] and Hweehua Pang[2]**

[1] *Information Security Laborator, Institute for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore 119613*
[2] *School of Information Systems, Singapore management University, Singapore 178902*

Correspondence should be addressed to Yongdong Wu, wydong@i2r.a-star.edu.sg

Received 4 March 2008; Revised 3 June 2008; Accepted 6 June 2008

Recommended by Chiou-Ting Hsu

The buyer-seller watermarking protocol enables a seller to successfully identify a traitor from a pirated copy, while preventing the seller from framing an innocent buyer. Based on finite field theory and the homomorphic property of public key cryptosystems such as RSA, several buyer-seller watermarking protocols (N. Memon and P. W. Wong (2001) and C.-L. Lei et al. (2004)) have been proposed previously. However, those protocols require not only large computational power but also substantial network bandwidth. In this paper, we introduce a new buyer-seller protocol that overcomes those weaknesses by managing the watermarks. Compared with the earlier protocols, ours is $n$ times faster in terms of computation, where $n$ is the number of watermark elements, while incurring only $O(1/l_N)$ times communication overhead given the finite field parameter $l_N$. In addition, the quality of the watermarked image generated with our method is better, using the same watermark strength.



## 1. INTRODUCTION

The rapid development of computer networks and increased use of multimedia data via the Internet have resulted in fast and convenient exchange of digital information. With the ease of editing and perfect reproduction, the protection of ownership of digital audio, image and video materials become an important concern. Copyright marking [1] is a relatively new technique for hiding information in multimedia content with the aim of tracing any traitor who redistributes the content illegally. Its application is broad, *for instance*, copyright protection [2–4].

In general, a watermarking scheme for traitor tracing (a traitor is a legitimate buyer who subsequently distributes his copy illegally) involves three steps: first, an owner embeds into a cover image a watermark that identifies the buyer. Secondly, if a suspicious image is found, the owner will detect the watermark in the image. Once the watermark of a specific buyer is identified, the owner will take the case to a court. Finally, the authority will independently detect the watermark again in the image in question. If the watermark is really found, the traitor is confirmed. A number of watermarking protocols have been proposed in [5–9] to track down the distributors of illegal replicas.

However, the accusation against the charged distributor, who was the buyer in some earlier transaction, could be objectionable because the seller also has access to the watermarked copies and, hence, is able to release such a replica on his own to frame the distributor.

To solve the `customer`'s right problem [10] in the arbitration phase, Memon and Wong [11] proposed an interactive buyer-seller protocol (hereafter referred to as MW protocol) for invisible watermarking. In the protocol, the seller does not know the watermark of the buyer, so the seller cannot create copies of the protected content containing the buyer's watermark. After the seller finds an unauthorized copy, the seller can identify the buyer from a watermark in the unauthorized copy, and furthermore the seller can prove this fact to a third party using a dispute resolution protocol. This prevents the buyer from claiming that the unauthorized copy may have originated from the seller himself. Memon and Wong proposed two embodiments in [11, 12] based on RSA [13] and ElGamal [14] crytosystems, respectively.

As explained in [15], Memon's protocol has a weakness in that the seller can frame a buyer with a higher-value image; this is known as `unbinding problem` in [15]. To rectify the problem, Lei et al. proposed another buyer-seller protocol (called LYTC protocol hereinafter), which inserts a second watermark into the cover image. The second watermark is generated by a watermark certification authority (WCA) and sent to the buyer securely. As further observed in [15, page 1620], "*the protocol* (note: [11]) *restricts itself to the use*

*of linear watermarking schemes and, hence, provides limited flexibility in practice*." However, Lei et al. did not propose any nonlinear method that would have allowed them to replace the asymmetric cipher in their protocol with a much cheaper symmetric cipher. Zhang et al. [16] enhanced the previous buyer-seller schemes with the same computational complexity so as to defeat malicious arbitrator. Recently, Zhao et al. [17] follow the footprint of MW scheme. It is not clear whether it is possible to design a nonlinear scheme because the popular/standard asymmetric cryptosystems are in finite fields. For example, other buyer-seller schemes such as [18] also employ asymmetric cipher. Hence the cover image has to be separated and encrypted independently in the previous schemes.

Neither MW nor LYTC is efficient in terms of computation cost and communication overhead, because a lot of asymmetric cipher operations are performed. As the buyer-seller protocol may be employed in an online application, for example a paid Internet image gallery, response time is important to user retention. In particular, the buyer may be using a mobile device that has only limited computing power, battery life, and/or communication bandwidth. Therefore, to be feasible in practice, an alternative light-weight buyer-seller protocol is needed.

Kuribayashi and Tanaka [19] proposed an anonymous fingerprinting that improves the enciphering rate with interactive Zero-knowledge proof. But it is computationally intensive and bandwidth inefficient.

In our proposed protocol, the seller asks a WCA to generate two independent watermarks $\mathbf{W}$ and $\widehat{\mathbf{W}}$, where $\mathbf{W}$ is used for identifying the buyer at the WCA side. Let $\mathbf{V} = \mathbf{W} + \beta\widehat{\mathbf{W}}$ where $\beta$ is a predefined parameter to ensure frame-proof. $\mathbf{V}$ is for the seller securely while $\widehat{\mathbf{W}}$ is for the buyer securely. To be able to identify the buyer with $\mathbf{V}$ at the seller side, the seller embeds $\mathbf{V}$ into the cover image to produce a watermarked image. The buyer obtains the watermarked image which she watermarks again with $(\beta\widehat{\mathbf{W}})$; this effectively reverses out $\beta\widehat{\mathbf{W}}$ and leaves the final copy that is watermarked with $\mathbf{W}$. The identification step is the same as that in [5]. While the proposed protocol may look similar to multiwatermarking schemes (e.g., [20, 21]) at first sight, our scheme is really different from them in nature. Specifically, the watermarks in multiwatermarking are independent and all the watermarked images are of high quality. In contrast, the watermarks $\mathbf{V}$ and $\widehat{\mathbf{W}}$ in our scheme are dependent, and only the final watermarked copy derived by the buyer is of high quality since one watermark alleviates the effect of the other.

The reminder of this paper is as follows. Section 2 elaborates on our protocol. Section 3 analyzes the protocol in terms of frame deterrence, performance comparison, and so forth. Section 4 describes experiment results. Finally, Section 5 concludes the paper.

## 2. THE PROPOSED BUYER-SELLER PROTOCOL

Denote the original image as $\mathbf{X} = \{x_1, x_2, \ldots, x_n\}$ and the watermarks for identifying a buyer as $\mathbf{W} = \{w_1, w_2, \ldots, w_n\}$ and $\widehat{\mathbf{W}} = \{\hat{w}_1, \hat{w}_2, \ldots, \hat{w}_n\}$, where $n$ is the number of image elements (e.g., DCT coefficients) to be manipulated. Our protocol is a light-weight buyer-seller watermarking scheme that focuses on managing the watermarks. We do not design a new embedding method, but simply employ a state-of-the-art scheme for embedding the watermarks. In particular, the robust watermarking method Add-embedding in [5] is used for illustrating our proposed solution

$$y_i = x_i + \alpha w_i, \quad i = 1, 2, \ldots, n, \tag{1}$$

where $\alpha$ is the watermark strength relating to watermark robustness and invisibility. $\mathbf{Y} = \{y_1, y_2, \ldots, y_n\}$ is the watermarked image.

### 2.1. Trust model

In our protocol, the trust model is the same as that in MW and LYTC. There are three participants: seller, buyer, and WCA. The seller may attempt to frame an innocent buyer with an image that is embedded with the buyer's watermark (`customer`'s right problem), or frame a traitor with a higher-value image (`unbinding problem`. ( `unbinding problem`: when a pirated copy is found and the illegal distributor is identified, a higher-value image enables the seller to seek much higher compensation from the illegal distributor.) The buyer may attempt to disseminate her legal copy without being identified (`traitor tracing problem`). In addition, the WCA, who is a trusted third party, is assumed to manage the watermarks secretly in the process of watermark generation, storage, delivery, and arbitration.

We also assume that the watermarks are independent and normalized. That is to say, for any pair of watermarks $\mathbf{W}_1$ and $\mathbf{W}_2$, $\mathbf{W}_1 \bullet \mathbf{W}_2 = 0$ if $\mathbf{W}_1 \neq \mathbf{W}_2$, otherwise 1, where $\bullet$ is the correlation operator (i.e., inner product).

For simplicity, for the rest of this paper we assume that all the communication messages are authentic and that the cover signal is an image.

### 2.2. Watermarking protocol

In the watermarking process, the original image is doubly-watermarked with the watermarks generated from a WCA. Figure 1 summarizes the message flows in the watermarking process.

(1) Acting on information such as advertisement or the seller's website, the buyer $B$ decides to purchase an image. She thus sends a request for the image.

(2) The seller $S$ generates a fingerprint $h_S$ from the original image from the features of original image $\mathbf{X}$ (e.g., [22]). He then forwards the request of the buyer along with $h_S$ to a WCA.

(3) The WCA generates two independent watermark sequences $\mathbf{W}$ and $\widehat{\mathbf{W}}$ based on $h_S$ and buyer's description. Let $\mathbf{V} = \mathbf{W} + \beta\widehat{\mathbf{W}}$, where $\beta > 1$ is a predefined parameter that controls the quality of the watermarked image at the seller side. The WCA sends the ciphertext $\mathcal{E}_B(\alpha\beta\widehat{\mathbf{W}})$ to the buyer, and $\mathcal{E}_S(\mathbf{V})$ to the seller respectively. (In order to speed

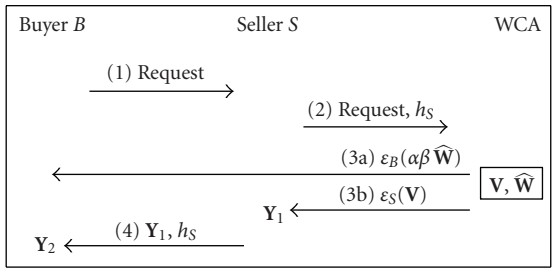



Figure 1: Our proposed watermarking protocol. $\mathbf{Y}_1$ is the seller's copy, and $\mathbf{Y}_2$ is the buyer's copy. $\mathcal{E}_B(\cdot)$ is a hybrid encryption [23] with the public key of buyer. $h_S$ is the fingerprint of the original image, and it is signed by the seller (the signature is not shown here).

up encryption/decryption, a hybrid algorithm [23] is used to produce $\mathcal{E}_S(\mathbf{V})$: WCA generates a random session key $K$, then encrypts $K$ with the seller's public key, and encrypts the watermark $\mathbf{V}$ with the session key $K$. A similar process is applied to produce $\mathcal{E}_B(\widehat{\mathbf{W}})$.)

(4) The seller decrypts $\mathcal{E}_S(\mathbf{V})$ to extract $\mathbf{V}$. Next he inserts $\mathbf{V}$ into the cover image $\mathbf{X}$ to produce his watermarked copy $\mathbf{Y}_1 = \mathbf{X} + \alpha\mathbf{V} = \mathbf{X} + \alpha(\mathbf{W} + \beta\widehat{\mathbf{W}})$. The seller sends $\mathbf{Y}_1$ and $h_S$ to the buyer.

(5) The buyer decrypts $\mathcal{E}_B(\alpha\beta\widehat{\mathbf{W}})$ with her private key to obtain $\alpha\beta\widehat{\mathbf{W}}$, then she generates her watermarked copy

$$\mathbf{Y}_2 = \mathbf{Y}_1 - \alpha\beta\widehat{\mathbf{W}} = \mathbf{X} + \alpha(\mathbf{W} + \beta\widehat{\mathbf{W}}) - \alpha\beta\widehat{\mathbf{W}} = \mathbf{X} + \alpha\mathbf{W}. \tag{2}$$

Afterwards, the buyer will reconstruct the fingerprint $h_B$ of $\mathbf{Y}_2$. Due to the invisibility property of watermarking, the original image is only manipulated slightly. Hence, $h_S$ should match the fingerprint $h_B$ at a very high probability. Thus, if $h_S \neq h_B$, the buyer rejects the watermarked image $\mathbf{Y}_2$ and complains to the WCA.

### 2.3. Identification protocol

Whenever the seller finds a suspicious copy $\mathbf{Y} = \mathbf{Y}_2 + \alpha\mathbf{D}$, where $\mathbf{D}$ is a distortion due to whatever reasons, he tests the copy with the buyer's message $\mathbf{V}$ based on the method in [5]. Specifically, he checks whether

$$\begin{aligned}\gamma_S &= (\mathbf{Y} - \mathbf{X})\bullet\frac{\mathbf{V}}{\alpha}\\ &= (\mathbf{W} + \mathbf{D})\bullet(\mathbf{W} + \beta\widehat{\mathbf{W}})\\ &\approx 1 + \mathbf{D}\bullet(\mathbf{W} + \beta\widehat{\mathbf{W}})\\ &\approx 1 + \epsilon > \eta_S\end{aligned} \tag{3}$$

for some predefined threshold $\eta_S$, where $\epsilon$ is a small number. Thus, the seller will accuse the buyer if $\gamma_S > \eta_S$. If there are more than one potential traitor, the seller may target the one with the largest $\gamma_S$.

### 2.4. Dispute resolving protocol

In case the buyer denies that an unauthorized copy originated from her version of the image, the seller asks the WCA (for simplicity, we assume that the WCA is also the arbitrator.) to resolve the dispute. Since the WCA calculates the correlation value with $\mathbf{W}$ instead of $\mathbf{V}$ according to (4), smaller noise is involved in WCA's detection. Hence the WCA's decision is final:

$$\begin{aligned}\gamma_W &= (\mathbf{Y} - \mathbf{X})\bullet\frac{\mathbf{W}}{\alpha}\\ &= (\mathbf{W} + \mathbf{D})\bullet\mathbf{W}\\ &\approx 1 + \mathbf{D}\bullet\mathbf{W}\\ &\approx 1 + \epsilon' > \eta_W,\end{aligned} \tag{4}$$

where $\epsilon'$ is small since $\mathbf{D}$ and $\mathbf{W}$ are independent.

## 3. ANALYSIS OF THE PROPOSED PROTOCOL

In this section, we analyze the proposed protocol with regards to customer's right, traitor tracing, and performance.

### 3.1. Parameter selection

The present scheme has to select some parameters, especially $\alpha$ and $\beta$. $\alpha$ is used to control the quality of the watermarked image generated by buyer, and $\beta$ is used to prevent the seller from framing the buyer. For the sake of security, both $\alpha$ and $\beta$ are unknown to the buyer. Based on (8) in Section 3.2, $\beta = 10$ is enough since the interference noise can reduce the quality of watermarked image 20 dB. The other parameters for threshold values (e.g., $\eta_S$ for seller's detection and $\eta_W$ for arbitrator's detection) can be decided based on the security requirement.

### 3.2. Frame-resilience

Since the seller knows the image $\mathbf{Y}_1$ which is watermarked with both $\mathbf{W}$ and $\widehat{\mathbf{W}}$, an accused buyer may argue that she has been framed by the buyer. Fortunately, the watermarked image $\mathbf{Y}_1$ that the seller possesses is of low quality due to the large amount of noise $\alpha(\mathbf{W} + \beta\widehat{\mathbf{W}})$, so it is not worth to protect the watermarked image $\mathbf{Y}_1$ at all. To demonstrate the fidelity of the watermarking, let us measure the distortion mean squared error (MSE) $\sigma_1$ and $\sigma_2$ of the watermarked images $\mathbf{Y}_1$ and $\mathbf{Y}_2$:

$$\sigma_1 = ||\mathbf{Y}_1 - \mathbf{X}||^2 = ||\alpha(\mathbf{W} + \beta\widehat{\mathbf{W}})||^2 \approx \alpha^2(1 + \beta^2), \tag{5}$$

$$\sigma_2 = ||\mathbf{Y}_2 - \mathbf{X}||^2 = ||\alpha\mathbf{W}||^2 \approx \alpha^2. \tag{6}$$

Therefore, the difference $\Delta_{\text{PSNR}}$ in peak signal-to-noise ratio (PSNR) [24] between $\mathbf{Y}_1$ and $\mathbf{Y}_2$ is

$$\begin{aligned}\Delta_{\text{PSNR}} &= \text{PSNR}_2 - \text{PSNR}_1\\ &= 10\log_{10}\frac{\sigma_1}{M} - 10\log_{10}\frac{\sigma_2}{M}\end{aligned} \tag{7}$$

$$\begin{aligned}&= 10\log_{10}\left(\frac{\alpha^2(1+\beta^2)}{M}\right) - 10\log_{10}\left(\frac{\alpha^2}{M}\right)\\ &= 10\log_{10}(1+\beta^2) > 20\log_{10}\beta\,(\text{dB}),\end{aligned} \tag{8}$$

where $M$ is the number of pixels in the image. To achieve high robustness, Cox's watermarking method in (1) is performed

in frequency domain, thus, (5) and (6) are calculated in frequency domain. However, PSNR is defined in spatial domain. We are still able to calculate the difference in PSNR with (7) though, because the MSE in spatial domain is equal to that in frequency domain. According to (8), the quality of the watermarked image $\mathbf{Y}_1$ is much lower than that of $\mathbf{Y}_2$. Therefore, the buyer is willing to execute the second embedding so as to reduce the embedding noise. Since $\mathbf{Y}_1$ is of very low quality, the seller has no reason to frame a buyer with such a poor-quality image.

### 3.3. Detecting malicious buyer

The identification protocol in Section 2.3 can detect a traitor if she follows the protocol faithfully. However, a malicious buyer may attempt to defeat the protocol by exploiting knowledge of the watermarked image $\mathbf{Y}_1$ and her watermark $\widehat{\mathbf{W}}$. For instance, the buyer selects a random sequence $\mathbf{Z}$ over a distribution with mean 1, and generates a new watermark $\alpha\beta\,\widehat{\mathbf{W}}'$ which is close to $\alpha\beta\,\widehat{\mathbf{W}}$:

$$\begin{aligned}\mathbf{Z} &= \{z_i \mid i = 1, 2, \ldots, n\},\\ \widehat{\mathbf{W}} &= \{\hat{w}_i \mid i = 1, 2, \ldots, n\},\\ \alpha\beta\,\widehat{\mathbf{W}}' &\stackrel{\text{def}}{=} \{\hat{w}_i' \mid \hat{w}_i' = z_i(\alpha\beta\,\hat{w}_i),\ i = 1, 2, \ldots, n\}.\end{aligned} \tag{9}$$

Then, she calculates

$$\mathbf{Y}_2' = \mathbf{Y}_1 - \alpha\beta\,\widehat{\mathbf{W}}' = \mathbf{X} + \alpha(\mathbf{W} + \beta\,\widehat{\mathbf{W}} - \beta\,\widehat{\mathbf{W}}'). \tag{10}$$

If the seller finds an illegal $\mathbf{Y}_2'$, he will check it with (3) as

$$\begin{aligned}\gamma_S &= (\mathbf{Y}_2' - \mathbf{X}) \bullet \frac{\mathbf{V}}{\alpha}\\ &= (\mathbf{W} + \beta\,\widehat{\mathbf{W}} - \beta\,\widehat{\mathbf{W}}') \bullet (\mathbf{W} + \beta\,\widehat{\mathbf{W}})\\ &= 1 + \beta^2 - \beta\,\widehat{\mathbf{W}}' \bullet (\mathbf{W} + \beta\,\widehat{\mathbf{W}})\\ &= 1 + \beta^2 - \beta^2\,\widehat{\mathbf{W}}' \bullet \widehat{\mathbf{W}}.\end{aligned} \tag{11}$$

Clearly, the correlation value $\gamma_S$ is a random variable which depends on variable $\mathbf{Z}$. Since $\alpha\beta$ is unknown to the buyer, $z_i$ should be selected by the buyer in a small interval $[1-\varepsilon, 1+\varepsilon]$. Therefore, the expected value of $\gamma_S$ is

$$E(\gamma_S) = E(1 + \beta^2 - \beta^2\,\widehat{\mathbf{W}}' \bullet \widehat{\mathbf{W}}) = 1 + \beta^2 - \beta^2 = 1. \tag{12}$$

In contrast, the expected correlation value $\gamma_S''$ of an innocent buyer with watermark pair $(\mathbf{W}'', \widehat{\mathbf{W}}'')$ is

$$\begin{aligned}\mathbf{V}'' &= \mathbf{W}'' + \beta\,\widehat{\mathbf{W}}'',\\ E(\gamma_S'') &= E\left((\mathbf{Y}_2' - \mathbf{X}) \bullet \frac{\mathbf{V}''}{\alpha}\right)\\ &= E((\mathbf{W} + \beta\,\widehat{\mathbf{W}} - \beta\,\widehat{\mathbf{W}}') \bullet (\mathbf{W}'' + \beta\,\widehat{\mathbf{W}}''))\\ &= -E(\widehat{\mathbf{W}}' \bullet (\mathbf{W}'' + \beta\,\widehat{\mathbf{W}}'')) = 0.\end{aligned} \tag{13}$$

Thus, a traitor can be identified at a high probability, while an innocent buyer has a very low probability of being accused wrongly.

Table 1: Performance comparison.

| | MW [11] | LYTC [15] | Present |
|---|---|---|---|
| MSE $\sigma$ | $2\alpha^2$ | $2\alpha^2$ | $\alpha^2$ |
| Seller time $t_S$ | $n(T_e + T_m)$ | $n(T_e + T_m)$ | $T_d$ |
| Buyer time $t_B$ | $nT_d$ | $nT_d + T_{sk}$ | $T_d$ |
| WCA time $t_W$ | $nT_e$ | $nT_e$ | $2T_e$ |
| Seller overhead $C_S$ | $nl_N$ | $nl_X + nl_N$ | $nl_X + l_N$ |
| WCA overhead $C_W$ | $nl_N$ | $nl_N$ | $2nl_W + 2l_N$ |

$T_e$: the computation time for an asymmetric encryption.
$T_d$: the computation time for an asymmetric decryption.
$T_m$: the computation time for a modular multiplication
$T_{sk}$: the computation time for generating a pair of public/private key. $T_{sk} \gg T_d$.
$n$: the number of DCT coefficients to be manipulated.
$l_X$: the size of one image element $x_i$.
$l_N$: the size of a RSA modulus $N$.
$l_W$: the size of one watermark element $w_i$.

Table 2: Example performance comparison

| | MW [11] | LYTC [15] | Present |
|---|---|---|---|
| Seller time (millisecond) | 1800 | 1800 | 4.77 |
| Buyer time (millisecond) | 47700 | 48177 | 4.77 |
| WCA time (millisecond) | 1800 | 1800 | 0.36 |

### 3.4. Performance comparison

In this subsection, we compare our protocol with the earlier protocols in [11, 15], in terms of computation cost and communication overhead. Here, Mul-RSA denotes the protocols in [11, 15]. Table 1 gives the comparative performance among the protocols. In the table, the first row indicates the quality degradation of the final watermarked image $\mathbf{Y}_2$ with reference to the original image $\mathbf{X}$. Clearly, our method (in (6)) produces watermarked images of better quality than that achievable by [11] or [15], with the same parameter $\alpha$.

In the previous schemes [11, 15], each element is processed independently, thus the computation cost and overhead increase linearly with the number $n$ of the manipulated elements. In contrast, our protocol which employs the hybrid scheme [23] has only one asymmetric operation at the seller/buyer, and two asymmetric operations at the WCA. Correspondingly, the communication overhead is almost constant. As a result, our scheme is much more efficient in terms of computation cost (rows 3–5) and communication overhead (rows 6-7). Roughly, the earlier schemes are $n$ times slower while generating $l_N/l_X$ times more network traffic.

To illustrate the performance differences, we use typical parameter settings $l_X = 64$, $l_N = 1024$, $l_W = 32$, and $n = 10000$. Since symmetric cipher (e.g., AES/RC4) is much faster (over 1000 times) than asymmetric cipher (e.g., RSA-1024), we can ignore the computation time of symmetric encryption/decryption. According to the experiment in [25] with Pentium IV 2.1 GHz processor running Windows XP, $T_e = 0.18$ millisecond, $T_d = 4.77$ millisecond, $T_{sk} \approx 100T_d = 477$ millisecond. As shown in Table 2, the protocols of [11, 15] are almost 360 times slower than our scheme at the seller,

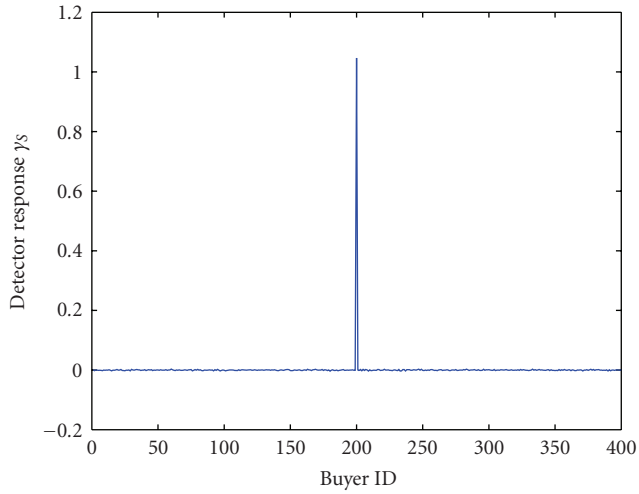



Figure 2: Identifying the "honest" buyer by the seller. The seller tests the buyers with the watermark **V** according to (3).

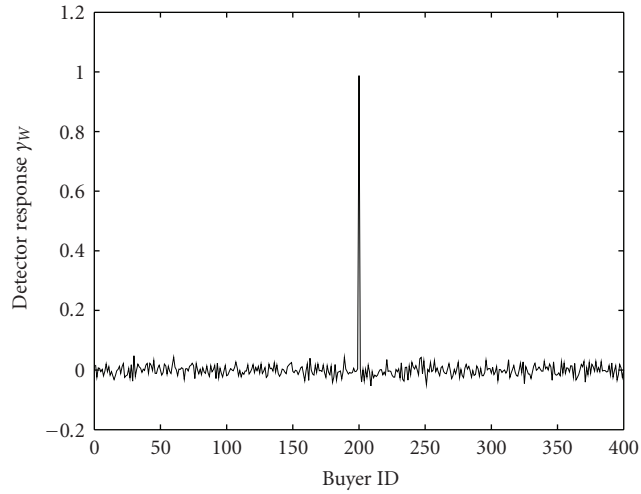



Figure 3: Identifying the "honest" buyer by the WCA. The WCA traces the traitor with the watermark **W** according to (4).

and 10000 times slower at the buyer. The latter differentiation is particularly critical for buyers that use portable devices with limited computing and communication resources.

We should also clarify that the proposed protocol has the disadvantage that the WCA (or seller) has to record all the watermarks **W** (or **V**, resp.) associated to each transaction, whereas in [15] only seller records the watermarks, and WCA is memoryless.

## 4. EXPERIMENTAL RESULTS

In the following experiments, we set $\alpha = 20$, $\beta = 10$, and the size of the test images to $200 \times 200$. The normalized watermarks **W** and $\widehat{\mathbf{W}}$ are of length $n = 1000$. For each $8 \times 8$ DCT block, 16 coefficients are selected for embedding. Thus, each watermark is embedded with the repetition $r = (200 \times 200/8 \times 8) \times 16/n = 10$ to achieve robustness in detection.

As our protocol aims to protect customer's right, it employs Cox's embedding method [5] twice and hence produces the watermarked images $\mathbf{Y}_1$ and $\mathbf{Y}_2$. The entire watermarking process includes the following steps. (1) The WCA produces watermarks **W** and $\widehat{\mathbf{W}}$. (2) The seller performs DCT on the original image **X**, embedding $\mathbf{V} = \mathbf{W} + \beta\widehat{\mathbf{W}}$ into **X** in the DCT domain, IDCT, and round IDCT output into integer interval [0, 255] to produce $\mathbf{Y}_1$. (3) The buyer executes DCT on $\mathbf{Y}_1$, embedding $\beta\widehat{\mathbf{W}}$ into $\mathbf{Y}_1$ in DCT domain, IDCT, and round IDCT output to produce $\mathbf{Y}_2$.

The following experiment results indicate that our protocol has little side-effect to the underlying embedding method in terms of robustness and invisibility.

### 4.1. Detecting "honest" traitor

To verify the detection method in Section 2.3, assume 400 watermark pairs $(\mathbf{W},\widehat{\mathbf{W}})$ are generated by the WCA, and assigned to 400 buyers. We generate a watermarked image $\mathbf{Y}_2$ with the watermarks of the 200th buyer according to (3). The seller then calculates the correlation values $\gamma_S$ with (3). Figure 2 illustrates the correlation values at the seller. It shows clearly that the 200th buyer is the traitor.

Similarly, Figure 3 shows the detection result of the WCA with (4). The WCA confirms that the 200th buyer is indeed the traitor.

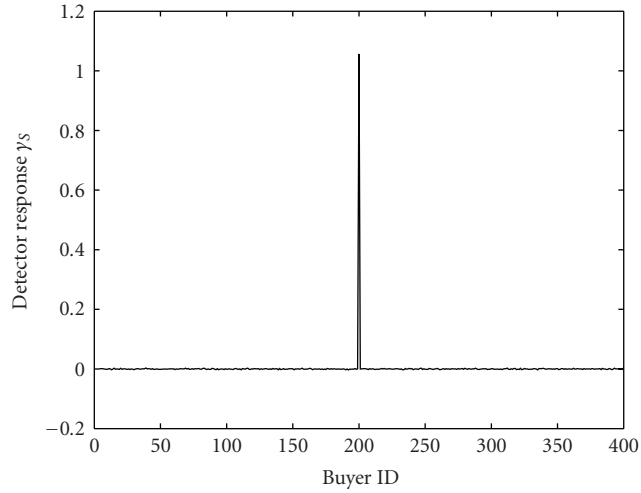



Figure 4: Identifying the malicious buyer by the seller. The seller tests the buyers with the watermark **V** according to (3).

### 4.2. Detecting malicious buyer

As mentioned in Section 3.3, a malicious buyer may use (10) instead of (3) to create a pirated copy. Assume that the buyer selects $z_i$ uniformly from $(0.9, 1.1)$ with mean 1. Since the watermark $\widehat{\mathbf{W}}'$ is close to $\widehat{\mathbf{W}}$, her watermarked image will be of good quality. If such a pirated copy is found, the seller calculates the correlation value $\gamma_S$ based on (3). Figure 4 illustrates the detection results by the seller for the traitor and

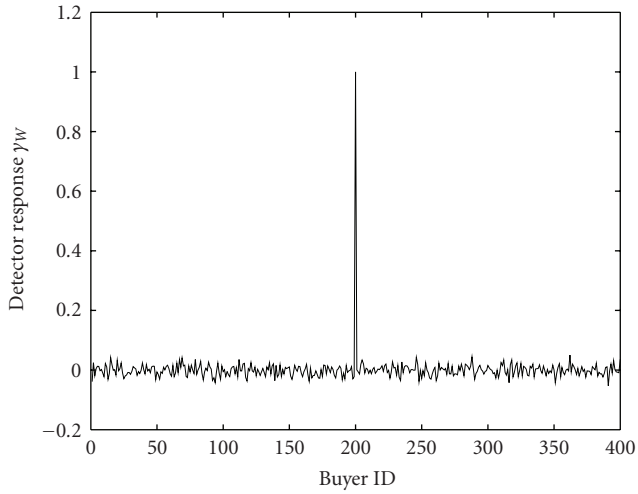



Figure 5: Identifying the malicious buyer by the WCA. The WCA traces the traitor with the watermark **W** according to (4).

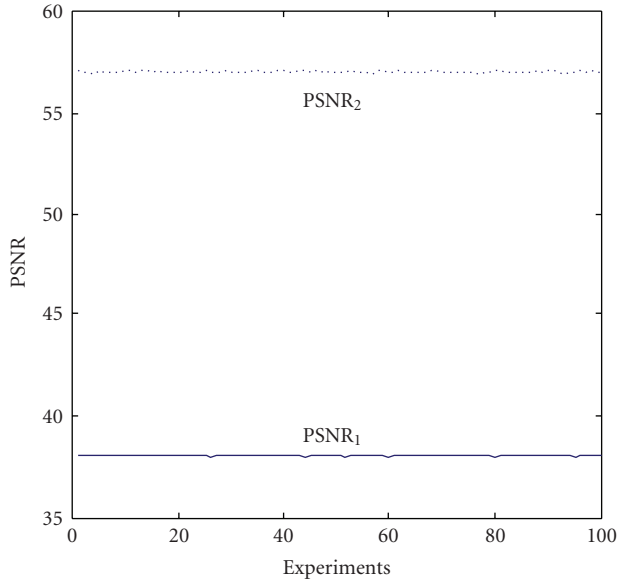


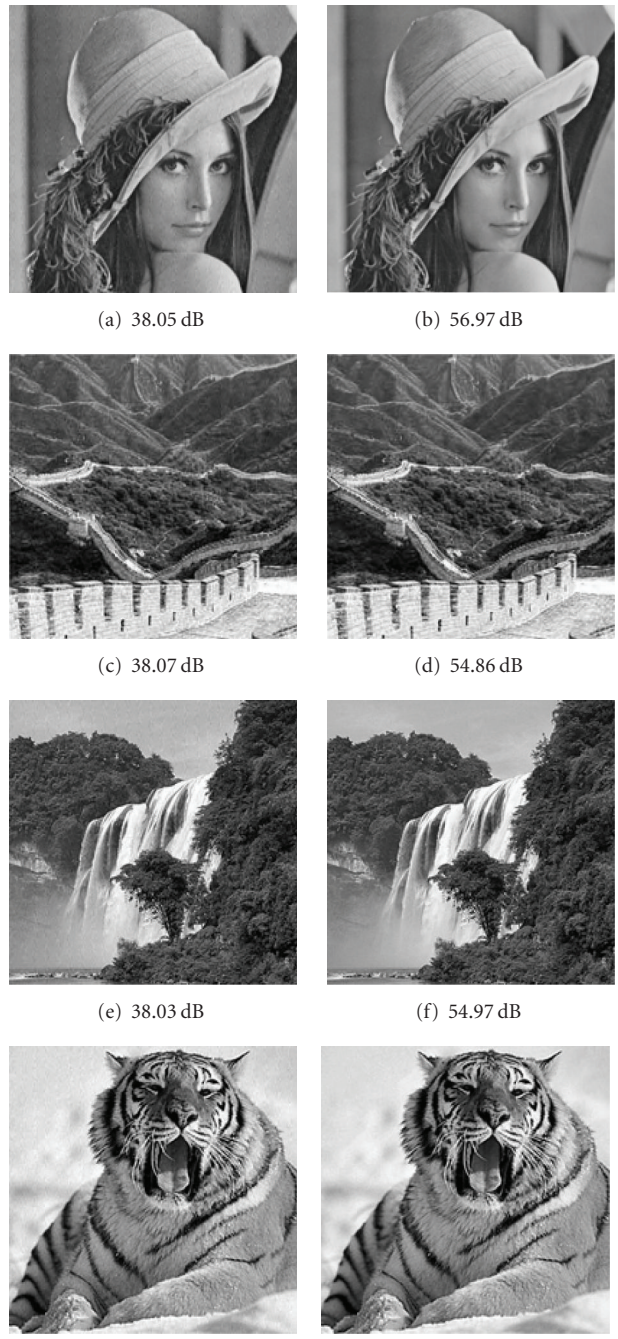

Figure 6: PSNR of $\mathbf{Y}_1$ and $\mathbf{Y}_2$.

innocent users. Similarly, Figure 5 is the detection result $\gamma_W$ from WCA according to (4).

As with "honest" traitors, the malicious buyer will be identified by the seller and WCA according to Figures 4 and 5. Therefore, the traitor is accused correctly while other buyers are not framed despite the traitor modifying the watermarking method. This experiment result is in concert with our analysis in (12) and (13).

### 4.3. Comparing PSNR of watermarked image

To demonstrate the different quality of the watermarked images, we now test a group of images. Figure 6 shows the PSNRs of the watermarked images, and Figure 7 shows a portion of the watermarked images $\mathbf{Y}_1$ and $\mathbf{Y}_2$. It is clear that



(a) 38.05 dB (b) 56.97 dB

(c) 38.07 dB (d) 54.86 dB

(e) 38.03 dB (f) 54.97 dB

(g) 38.11 dB (h) 54.17 dB

Figure 7: The watermarked images generated by the seller (left column) and buyer (right column), respectively.

the PSNR of $\mathbf{Y}_1$ is 16 dB lower than that of $\mathbf{Y}_2$; (due to integer transform, the experimental $\Delta_{\text{PSNR}}$ is smaller than that in (8)), this confirms that it is pointless for the seller to frame the buyer with $\mathbf{Y}_1$.

## 5. CONCLUSION

Since the buyer-seller protocols in [11, 15] employed the homomorphic property of public key cryptosystem to

encrypt each image element (i.e., DCT coefficient), they incur large computation costs and increase the size of the intermediate (encrypted) images (i.e., the first watermarked image). To overcome these shortcomings, we propose a watermark management solution that preserves the functionality in [11, 15], but is much more efficient in terms of computation cost and communication overhead. Another advantage is that watermarked images generated by our solution have significantly higher quality than that achievable by [11] or [15].

## REFERENCES


[1] F. Mintzer and G. W. Braudaway, "If one watermark is good, are more better?" in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '99)*, vol. 4, pp. 2067–2069, Phoenix, Ariz, USA, March 1999.

[2] C.-S. Lu and H.-Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1579–1592, 2001.

[3] C.-S. Lu, S.-K. Huang, C.-J. Sze, and H.-Y. M. Liao, "Cocktail watermarking for digital image protection," *IEEE Transactions on Multimedia*, vol. 2, no. 4, pp. 209–224, 2000.

[4] F. Ahmed, F. Sattar, M. Y. Siyal, and D. Yu, "A secure watermarking scheme for buyer-seller identification and copyright protection," *EURASIP Journal on Applied Signal Processing*, vol. 2006, Article ID 56904, 15 pages, 2006.

[5] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

[6] S. Craver, N. Memon, B.-L. Yeo, and M. M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 573–586, 1998.

[7] Y. Wang, J. F. Doherty, and R. E. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images," *IEEE Transactions on Image Processing*, vol. 11, no. 2, pp. 77–88, 2002.

[8] A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "A watermarking technique for the protection of digital images IPR," in *Advances in Information Technologies: The Business Challenge*, pp. 636–643, IOS Press, Amsterdam, The Netherlands, 1998.

[9] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1593–1601, 2001.

[10] 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, 1998.

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

[12] N. D. Memon and P. W. Wong, "Buyer-seller watermarking protocol based on amplitude modulation and the El Gamal Public Key Crypto System," in *Security and Watermarking of Multimedia Contents*, vol. 3657 of *Proceedings of SPIE*, pp. 289–294, San Jose, Calif, USA, January 1999.

[13] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[14] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, chapter 8, CRC Press, Boca Raton, Fla, USA, 1996.

[15] 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.

[16] J. Zhang, W. Kou, K. Fan, and L. Ye, "Watermarking protocol of secure verification," *Journal of Electronic Imaging*, vol. 16, no. 4, Article ID 043002, 4 pages, 2007.

[17] B. Zhao, W. Kou, J. Zhang, and K. Fan, "A watermarking scheme in the encrypted domain for watermarking protocol," in *Proceedings of the 3rd SKLOIS Conference on Information Security and Cryptology (Inscrypt '07)*, Xining, China, August-September 2007.

[18] B.-M. Goi, R. C.-W. Phan, Y. Yang, F. Bao, R. H. Deng, and M. U. Siddiqi, "Cryptanalysis of two anonymous buyer-seller watermarking protocols and an improvement for true anonymity," in *Proceedings of the 2nd International Conference on Applied Cryptography and Network Security (ACNS '04)*, vol. 3089 of *Lecture Notes in Computer Science*, pp. 369–382, Yellow Mountain, China, June 2004.

[19] M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," *IEEE Transactions on Image Processing*, vol. 14, no. 12, pp. 2129–2139, 2005.

[20] H. Guo and N. D. Georganas, "Digital image watermarking for joint ownership," in *Proceedings of the 10th ACM International Conference on Multimedia*, pp. 362–371, Juan-les-Pins, France, December 2002.

[21] P. H. W. Wong, O. C. Au, and Y. M. Yeung, "Novel blind multiple watermarking technique for images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 813–830, 2003.

[22] E.-C. Chang, S. Mallat, and C. Yap, "Wavelet foveation," *Applied and Computational Harmonic Analysis*, vol. 9, no. 3, pp. 312–335, 2000.

[23] F. Bao, R. Deng, P. Feng, Y. Guo, and H. Wu, "Secure and private distribution of online video and some related cryptographic issues," in *Proceedings of the 6th Australasian Conference on Information Security and Privacy (ACISP '01)*, vol. 2119 of *Lecture Notes in Computer Science*, pp. 190–205, Sydney, Australia, July 2001.

[24] D. S. Taubman and M. W. Marcellin, *JPEG2000: Image Compression Fundamentals, Standard and Practice*, Kluwer Academic Publishers, Dordrecht, The Netherlands, 2001.

[25] D. Wei, Crypto++ 5.2.1 Benchmarks, http://www.eskimo.com/~weidai/benchmarks.html.