ANONYMOUS BUYER-SELLER WATERMARKING PROTOCOL WITH ADDITIVE HOMOMORPHISM

Mina Deng, Li Weng
IBBT-COSIC, K. U. Leuven, ESAT/SCD, Kasteelpark Arenberg 10, bus 2446, B-3001 Leuven-Heverlee, Belgium

Bart Preneel
IBBT-COSIC, K. U. Leuven, ESAT/SCD, Kasteelpark Arenberg 10, bus 2446, B-3001 Leuven-Heverlee, Belgium

Keywords: Security, Watermarking protocol, e-Commerce, Cryptography.

Abstract: Buyer-seller watermarking protocols integrate multimedia watermarking and fingerprinting with cryptography, for copyright protection, piracy tracing, and privacy protection. We propose an efficient buyer-seller watermarking protocol based on dynamic group signatures and additive homomorphism, to provide all the required security properties, namely traceability, anonymity, unlinkability, dispute resolution, non-framing, and non-repudiation. Another distinct feature is the improvement of the protocol's utility, such that the double watermark insertion mechanism is avoided; the final quality of the distributed content is improved; the communication expansion ratio and computation complexity are reduced, comparing with conventional schemes.

1 INTRODUCTION

Today's information technology permits perfect duplication and cheap distribution for digital works. Copyright protection has become an important issue. In the realm of security, encryption and digital watermarking are recognized as promising techniques for copyright protection. *Encryption* is used to provide confidentiality. The limitation is that once the content is decrypted, it doesn't prevent illegal replications by an authorized user. *Digital watermarking*, complementing encryption, provides provable copyright ownership by imperceptibly embedding the seller's information in a digital content. Similarly, *fingerprinting* is used to identify copyright violators by embedding the buyer's information in the digital content.

The fingerprinting literature can be categorized as: fingerprinting for generic data, such as c-secure code by Boneh et al. (Boneh and Shaw, 1995), fingerprinting for multimedia data (Wang et al., 2005; Trappe et al., 2003; Liu et al., 2005), and fingerprinting protocols, such as those base on secure two-party computations (Pittzmann and Schunter, 1996; Pfitzmann and Waidner, 1997) or coin-based constructions (Pfitzmann and Sadeghi, 1999; Pfitzmann and Sadeghi, 2000; Camenisch, 2000). The shortcoming of these fingerprinting schemes is implementation inefficiency (Ju et al., 2002). On the other hand, the literature can also be categorized as: symmetric schemes, asymmetric schemes, and anonymous schemes. In *symmetric schemes* (Blakley et al., 1985; Boneh and Shaw, 1995; Cox et al., 1997), both the seller and the buyer know the watermark and the watermarked content. As a consequence, it is possible for a malicious seller to frame an innocent buyer, or an accused buyer to repudiate the guilt. This *customer's rights problem* in symmetric schemes was first pointed out by Qiao and Nahrstedt (Qiao and Nahrstedt, 1998). The problem can be solved by *asymmetric schemes* (Pittzmann and Schunter, 1996; Pfitzmann and Waidner, 1997; Biehl and Meyer, 1997), where only the buyer knows the final watermarked content, and hence the seller cannot fabricate piracy. To provide the buyer's anonymity, *anonymous schemes* (Pfitzmann and Sadeghi, 1999; Pfitzmann and Sadeghi, 2000) further use a registration service to eliminate the need of exposing the buyer's identity to the seller.

A buyer-seller watermarking protocol combines encryption, digital watermarking and fingerprinting, to ensure copyrights protection, privacy, and security for both the buyer and the seller simultaneously. The following security properties should be provided:

Traceability: A copyright violator should be able to be traced and identified.

Deng M., Weng L. and Preneel B. (2008).
ANONYMOUS BUYER-SELLER WATERMARKING PROTOCOL WITH ADDITIVE HOMOMORPHISM.
In *Proceedings of the International Conference on Signal Processing and Multimedia Applications*, pages 300-307
DOI: 10.5220/0001934303000307

Non-framing: Nobody can accuse an honest buyer.
Non-repudiation: A guilty buyer cannot deny his responsibility for a copyright violation caused by him.
Dispute resolution: The copyright violator should be identified and adjudicated without him revealing his private information, e.g. private keys or watermark.
Anonymity: A buyer's identity is undisclosed until he is judged to be guilty.
Unlinkability: Nobody can determine whether two watermarked contents are purchased by the same buyer or not.

The first known asymmetric buyer-seller watermarking protocol was introduced by Memon and Wong (Memon and Wong, 2001) by applying privacy homomorphic cryptosystems, and it was extended by Ju et al. (Ju et al., 2002). Since the introduction of the concept, several alternative designs have been proposed (Jae-Gwi Choi, 2003; Goi et al., 2004; Lei et al., 2004; Zhang et al., 2006; Ibrahim et al., 2007). Choi et al. (Jae-Gwi Choi, 2003) pointed out the *conspiracy problem* in (Memon and Wong, 2001; Ju et al., 2002), where a malicious seller can collude with an untrustworthy third party to fabricate piracy to frame an innocent buyer. Goi et al. (Goi et al., 2004) found the conspiracy problem couldn't be solved through commutative cryptosystems in (Jae-Gwi Choi, 2003). Lei et al. (Lei et al., 2004) addressed *the unbinding problem* in (Memon and Wong, 2001; Ju et al., 2002; Jae-Gwi Choi, 2003; Goi et al., 2004) and provided a mechanism to bind a specific transaction of a digital content to a specific buyer, such that a malicious seller cannot transplant the watermark embedded in a digital content to another higher-priced content. Zhang et al. (Zhang et al., 2006) presented a scheme, derived from (Lei et al., 2004), where no trusted third party (TTP) is required in the watermark generation phase and the conspiracy problem is solved. Unfortunately, we find the existence of *dispute resolution problem*: in (Zhang et al., 2006), in order to resolve disputes the buyer is required to cooperate and reveal his secret key or his secret watermark to the judge or to the *CA*, which is unrealistic in real-life applications. Ibrahim et al. (Ibrahim et al., 2007) recently proposed a scheme claiming that all the above problems has been solved.

In this paper, we propose a new anonymous buyer-seller watermarking protocol. Different from predecessors, our improvements are as follows:

Group Signature. Traceability, anonymity and unlinkability properties are essentially provided by deployment of group signature. We assume that a public key infrastructure *PKI* is available, such that each party has a public and private key pair certified by the *CA*. The *CA* is trustworthy and maintains the link between the buyer's private key and identity.

Support Multi-transactions. The buyer needs to register at the *CA* once before transactions, and there can be multiple transactions with the seller.

Avoid Double Watermark Insertion. Existing schemes all require double watermark insertions, and it has the drawback to cause a degradation of the final quality of the distributed contents, thus end up reducing their commercial value. When applied independently, the second watermark could confuse or discredit the authority of the first watermark, thus acting as an actual "ambiguity attack" (Frattolillo, 2007). We avoid it by designing a composite watermark, which is composed of the buyer's secret watermark, the seller's secret watermark, and a transaction index.

No Linear Watermark Limitation. The protocol is not limited to linear or permutation tolerant watermarks. As long as privacy homomorphism is preserved, any types of watermarking schemes can be adopted.

The rest of the paper is organized as follows. A model of anonymous buyer-seller watermarking protocol is defined in Sect. 2. The proposed protocol is explained in Sect. 3, with an example illustrated in Sect. 4. The protocol's security is analyzed in Sect. 5. Sect. 6 provides a conclusion.

2 PROTOCOL MODEL

Let $X_0 \in \{0,1\}^*$ be the cover data, $\mathbb{X}$ be the set of watermarked copies of X_0, and k be a security parameter. An anonymous buyer-seller watermarking protocol involves four parties: a seller and the copyright holder Alice $\mathcal{A}$, a buyer Bob $\mathcal{B}$, a certificate authority *CA* that functions as a group manager, and a judge $\mathcal{J}$ that adjudicates lawsuits against the infringement of copyrights. It consists of three subprotocols.

`Reg-BCA`: The registration protocol consists of an algorithm `Set-CA` and a protocol `Reg`. `Set-CA` is a probabilistic key setup algorithm to generate the *CA*'s public key gpk and private keys (ok, ik). `Reg` is a probabilistic two-party protocol `(Reg-CA, Reg-B)` between the *CA* and $\mathcal{B}$. Their common input are $\mathcal{B}$'s identity B and gpk. The *CA*'s secret input is (ok, ik). $\mathcal{B}$'s output is his group signature key gsk_B. The *CA* stores $\mathcal{B}$'s certificate $cert_B$ and identity B in a registration table as $reg[B]$.

`WK-BS`: A two-party protocol `(WK-S,WK-B)` between $\mathcal{A}$ and $\mathcal{B}$. Their common input is gpk. $\mathcal{A}$'s secret input are the cover data X_0 and a transaction number ϕ, and $\mathcal{A}$'s output is a transaction record in $Table_A$.

Table 1: Notations and abbreviations.

B	Buyer's identification information
X_0	Original content
$\mathbb{X}$	The set of watermarked content of X_0
$X^{'}$	A watermarked content of X_0, $X^{'} \in \mathbb{X}$
$\mathtt{Det}(X_0, Y)$	Non-blind watermark extraction
ARG	Transaction agreement
$E_{pk_i}(\cdot)$	Encryption with the public key of i
$D_{sk_i}(\cdot)$	Decryption with the private key of i
(pk_B, sk_B)	$\mathcal{B}$'s verification and signing keys
(pk_B^*, sk_B^*)	$\mathcal{B}$'s one-time anonymous key pair
sig_B	$\mathcal{B}$'s signature to pk_B signed with upk_B
$cert_B$	$\mathcal{B}$'s certificate from the issuer.
gsk_B	$\mathcal{B}$'s group signature key
$reg[i]$	Registration table of group member i
1^k	For $k \in \mathbb{N}$, the string of k ones.
μ	$\mathcal{B}$'s group signature to pk_B^*
$E_{esc}, pf_{sk_B^*}$	$\mathcal{B}$'s key escrow cipher and its proof
W_A	Seller's secret watermark
W_B	Buyer's secret watermark
ϕ	Index of seller's transaction record
ε	Empty string

$\mathcal{B}$'s secret input is $\mathcal{B}$'s group signature key gsk_B, and $\mathcal{B}$'s output is a watermarked copy $X^{'} \in \mathbb{X}$.

`Arb-SJCA`: A three-party protocol (`Arb-S`, `Arb-J`, `Arb-CA`) among $\mathcal{A}$, $\mathcal{J}$, and the *CA*. $\mathcal{A}$ and $\mathcal{J}$'s input are a pirated copy $Y \in \mathbb{X}$, the cover data X_0, and a record in $Table_A$. The *CA*'s input are (gpk, ok, ik) and the list of $cert_B$'s in *reg*. The *CA*'s output is the identity *id* of a buyer with a proof τ. $\mathcal{J}$ verifies τ and provides $\mathcal{A}$ the *id* or an empty string ε in case of failure.

The registration protocol `Reg-BCA` is performed once in the setup-phase by the *CA* for each new buyer. The watermarking protocol `WK-BS` is executed multiple times for multiple transactions between the buyer and the seller. The arbitration protocol `Arb-SJCA` is executed for dispute resolution.

3 PROPOSED SCHEME

In this section, we elaborate on the three subprotocols. We assume the *CA* is trustworthy and consists of a group key generator, an issuer for group member joining, and an opener for group signature opening. Note that the protocol's security depends on the security of the underlying watermarking and cryptographic primitives. As a consequence, the watermarking scheme employed is required to be collusion resistant. In particular, no colluded parties can remove or tamper the watermarking scheme, and nobody is able to detect or delete the embedded watermark from a content without knowing the watermark. As an example, we employ Bellare et al.'s dynamic group signature (Bellare et al., 2005), and Camenisch et al.s verifiable encryption scheme (Camenisch and Damgård, 1998) for key escrow of the buyers private key at the *CA*. Notations are depicted in Table 1.

3.1 Registration Protocol

The registration protocol performed between the buyer $\mathcal{B}$ and the *CA* is depicted in Fig.1. The *CA* executes the *group-key generation* algorithm `GKg` to produce the group public key gpk, the issuer key ik, and the opener key ok. Then $\mathcal{B}$ begins with the *user-key generation* algorithm `UKg` to obtain a key pair (upk_B, usk_B). To join the group, $\mathcal{B}$ generates a key pair (sk_B, pk_B), signs pk_B with usk_B resulting sig_B, and sends (pk_B, sig_B) to the issuer of the *CA*. If sig_B is verified, the *CA* issues $\mathcal{B}$ a certificate $cert_B$. Then (pk_B, sig_B) are stored in a registration table $reg[B]$, and sig_B can be used later by the opener to prove opening claims. Otherwise, the issuer returns an empty string ε and the protocol halts. Upon receiving $cert_B$, $\mathcal{B}$ generates his private group signature key gsk_B from the tuple $(B, pk_B, sk_B, cert_B)$.

3.2 Watermark Generation and Embedding Protocol

The watermarking protocol between the seller $\mathcal{A}$ and the buyer $\mathcal{B}$ is depicted in Fig.2. $\mathcal{A}$ and $\mathcal{B}$ first negotiate an agreement ARG on rights and specifications of a digital content X_0. After generating a one-time key pair (pk_B^*, sk_B^*), $\mathcal{B}$ executes the *group signing* algorithm `GSig` to create a signature μ to pk_B^*, as $\mu = \mathtt{GSig}(gpk, gsk_B, pk_B^*)$. Next, $\mathcal{B}$ computes an escrow cipher $E_{esc} = E_{pk_{RC}}(sk_B^*)$, to recover sk_B^* from the *CA* in case of disputes. The verifiable proof $pf_{sk_B^*}$ assures $\mathcal{A}$ that E_{esc} is valid without compromising the secret key sk_B^*. $\mathcal{B}$ generate a secret watermark W_B and encrypts W_B as $ew_B = E_{pk_B^*}(W_B)$. $\mathcal{B}$ sends $(pk_B^*, \mu, ARG, ew_B, pf_{sk_B^*}, E_{esc})$ and a signature λ to $\mathcal{A}$.

After $\mathcal{A}$ verifies $\mathcal{B}$'s group signature μ using gpk with the *group signature verification* algorithm `GVf`, she generates a secret watermark W_A, and an index ϕ to locate this transaction record in $Table_A$. Let $W_{AB} = W_A + W_B$, $W = W_{AB} + \phi 2^n$. W consists of the n-bit W_{AB} and the ℓ-bit ϕ. W can be decomposed into $\ell + n$

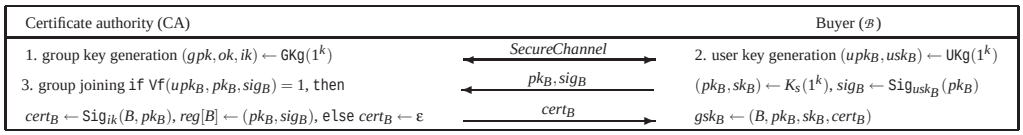


Figure 1: The registration protocol `Reg-BRC.` performed between the buyer $\mathcal{B}$ and the certificate authority *CA*.

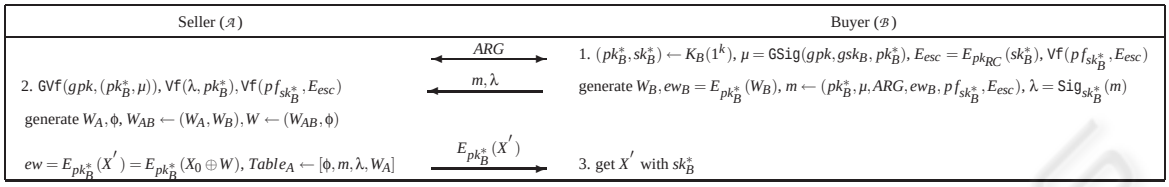


Figure 2: The watermark generation and embedding protocol `WK-BS.` performed between the seller $\mathcal{A}$ and the buyer $\mathcal{B}$.

binary numbers, with $W_i, W_{ABi}, \phi_i \in \{0,1\}$, satisfying:

$$W = \sum_{i=0}^{n+\ell-1} W_i 2^i = \sum_{i=0}^{n-1} W_{ABi} 2^i + \sum_{j=n}^{n+\ell-1} \phi_j 2^j \quad (1)$$

$$W_{AB} = \sum_{i=0}^{n-1} W_{ABi} 2^i \quad (2)$$

$$\phi = \sum_{j=0}^{\ell-1} \phi_j 2^j \quad (3)$$

$\mathcal{A}$ embeds the watermark in the encrypted domain, with additive homomorphism, $\mathcal{E}(\cdot)$ denotes $E_{pk_B^*}(\cdot)$:

$$\begin{aligned} \mathcal{E}(W) &= \mathcal{E}(W_A + W_B + \phi 2^n) \\ &= \mathcal{E}(W_A) \cdot \mathcal{E}(W_B) \cdot \mathcal{E}(\phi 2^n) \end{aligned} \quad (4)$$

$$\mathcal{E}(X') = \mathcal{E}(X_0) \otimes \mathcal{E}(W) = \mathcal{E}(X_0 \oplus W) \quad (5)$$

Thereafter, $\mathcal{A}$ stores (ϕ, m, λ, W_A) in $Table_A$, and delivers $E_{pk_B^*}(X')$ to $\mathcal{B}$. As a result, $\mathcal{B}$ obtains the watermarked content X' by decryption $D_{sk_B^*}(E_{pk_B^*}(X'))$.

3.3 Identification and Arbitration Protocol

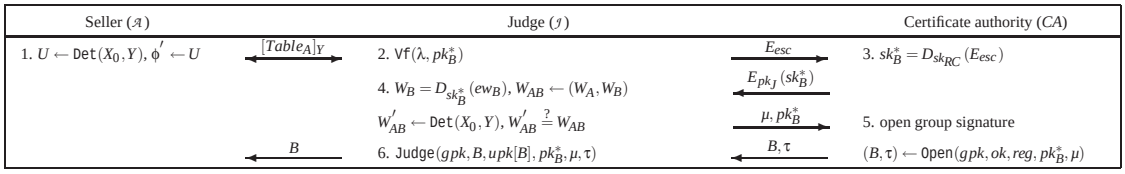
The identification and arbitration protocol among the seller $\mathcal{A}$, the judge $\mathcal{J}$, and the *CA*, is depicted in Fig. 3. Once a pirated copy Y of X_0 is found, $\mathcal{A}$ extracts the watermark U from Y and retrieves the most significant ℓ bits of U as the index ϕ' in order to search the $Table_A$. It is accomplished by choosing the value ϕ from $Table_A$ that is most correlated with ϕ'. Then, $\mathcal{A}$ provides the collected information to $\mathcal{J}$.

If λ is verified with the provided key pk_B^*, $\mathcal{J}$ sends the escrow cipher E_{esc} to the *CA*. Otherwise, the protocol halts. Next, the *CA* decrypts E_{esc} to recover the suspected buyer's private key $sk_B^* = D_{sk_{RC}}(E_{esc})$, and sends $E_{pk_J}(sk_B^*)$ back to $\mathcal{J}$. $\mathcal{J}$ recovers $sk_B^* = D_{sk_J}(E_{pk_J}(sk_B^*))$, $W_B = D_{sk_B^*}(ew_B)$, and calculates W_{AB} from W_A and W_B provided by $\mathcal{A}$. Meanwhile, $\mathcal{J}$ extracts the watermark U' from the pirated copy Y and retrieve the n least significant bits of U' as W'_{AB}. If W'_{AB} and W_{AB} match with a high correlation, the suspected buyer is proven to be guilty. Otherwise, the buyer is innocent. Note that until now, the buyer has stayed anonymous. To recover the buyer's identity, $\mathcal{J}$ orders the opener of the *CA* to execute the *group signature open* algorithm `Open`, to retrieve the identity B with a claim proof τ. $\mathcal{J}$ verifies B and τ with the *group signature judging* algorithm `Judge`. If verified, $\mathcal{J}$ adjudicates that the buyer with identity B is guilty. Otherwise, the protocol halts.

4 SCHEME EXAMPLE

In this section, we provide an example of the proposed protocol and employ the additive homomorphism of Damgård-Jurik cryptosystem (Jurik, 2001) and the watermarking scheme by Kuribayashi and Tanaka (Kuribayashi and Tanaka, 2005). Note that anti-collusion fingerprintings by Wu et al. (Wang et al., 2005; Trappe et al., 2003; Liu et al., 2005) can be applied for the coding of watermark values, in order to prevent complete removal or tampering of the watermarking by colluded parties. In this section, we focus on the watermarking embedding and detection scheme, but we will not explain anti-collusion fingerprints further.

The probabilistic encryption function of Damgård-Jurik cryptosystem (Jurik, 2001) is $\mathcal{E} : \mathbb{G} \rightarrow \mathbb{Z}^*_{n^{s+1}}$, with $\mathbb{Z}^*_{n^{s+1}} \cong \mathbb{G} \times \mathbb{H}$, $\mathbb{G}$ a cyclic group of order n^s, and $\mathbb{H} \cong \mathbb{Z}^*_n$. Choose an RSA modulus $n = pq$ and $s \in \mathbb{N}$. Choose $\lambda = lcm(p-1, q-1)$; $g \in \mathbb{Z}^*_{n^{s+1}}$ such that $g = (1+n)^j x \mod n^{s+1}$ for $gcd(j,n) = 1$ and $x \in \mathbb{H}$; $d \mod n \in \mathbb{Z}^*_n$ and $d \equiv 0$



Note: $\mu = \mathtt{GSig}(gpk, gsk_B, pk_B^*)$

Figure 3: The copyright violator identification and arbitration protocol `Arb-SJRC.` performed among $\mathcal{A}$, $\mathcal{J}$, and the *CA*.

mod λ (using the *Chinese Remainder Theorem*). The public key is (n, g), the private key is d. Given a plaintext $m \in \mathbb{Z}_{n^s}$, choose a random $r \leftarrow^R \mathbb{Z}^*_{n^{s+1}}$, and the ciphertext is $c = g^m r^{n^s} \mod n^{s+1}$. In decryption, given a ciphertext c, first compute $c^d \ mod \ n^{s+1} = (1+n)^{jmd \ mod \ n^s}$. Let $L(b) = (b-1)/n$, and jmd is obtained by applying a recursive version of Paillier's decryption scheme (Paillier, 1999). Since jd is known, $m = (jmd).(jd)^{-1} \mod n^s$.

The watermark $W = W_B + W_A + \phi 2^n$ is a binary vector $W = \{w_1, w_2, ..., w_m\}$, with $w_i = w_{Bi} + w_{Ai} + \phi_i 2^n \in \{0, 1\}$. Note that in order to be collusion resistant, W is embedded into m low frequency *DCT* coefficients $\{x_1, x_2, ..., x_m\}$ of the host image by the following basic steps:

1. Divide the image into 16×16 non-overlapping blocks;
2. Transform each block by two-dimensional DCT;
3. Quantize each block;
4. Embed the watermark by adjusting least significant bits of chosen DCT coefficients in each block;
5. Inverse transform each block.

The 16×16 quantization matrix Q is expanded from the standard 8×8 JPEG quantization matrix by a procedure introduced in (Kuribayashi and Tanaka, 2005). In order to adjust the embedding strength, a parameter q_w is defined. The final quantization matrix Q' is derived from Q according to:

$$Q'_{x,y} = \frac{100 - q_w}{50} Q_{x,y} \ .$$

To increase security, a few DCT coefficients in each block are chosen secretly for watermark embedding. Their indices are generated by a secure pseudo-random number generator according to a secret key. For each block, the candidate DCT coefficients are chosen from a limited low frequency band, as shown in Figure 4. In the simulation, the low frequency band is from $f_1 = 0.2$ to $f_2 = 0.6$ (normalized frequency). The embedding method is modifying the least significant bit (LSB) of a DCT coefficient after quantization. Conventional LSB-based watermarking methods modify the LSB in such a way that if watermark bit is 1, then the LSB is made odd, otherwise even. This approach cannot be directly used here because the watermark is encrypted and thus unknown to the embedder. Instead, some modification is made, as proposed by (Kuribayashi and Tanaka, 2005). A DCT coefficient is always quantized to the nearest even integer if it is chosen to embed one bit. To insert the watermark in the encrypted domain, we apply the additive homomorphism of (Jurik, 2001) over $m \in \mathbb{Z}_{n_s}$,

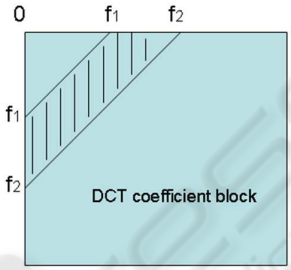


Figure 4: Frequency band for watermark embedding.

$$\begin{aligned} \mathcal{E}(m_1) \cdot \mathcal{E}(m_2) &= g^{m_1+m_2}(r_1 r_2)^{n^s} \mod n^{s+1} \\ &= \mathcal{E}(m_1 + m_2) \end{aligned} \quad (6)$$

In order to preserve the image quality, if the *re-quantized* DCT coefficient is larger than the original one, the watermark bit is subtracted from the quantized coefficient in the encrypted domain, otherwise it is added to the quantized coefficient. In order to increase robustness, the same watermark message is embedded repetitively for α times in the same image. After watermark detection, a majority voting is used to decide the watermark bit. Watermark detection is straightforward: each image block is transformed by DCT and then quantized; if the specified coefficient is even after quantization, the embedded bit is 0, otherwise it is 1.

Simulation is carried out to show the performance of this watermarking scheme. A 512×512 gray scale Lena image is used in the simulation, as shown in Figure 6(a). Assuming that the watermark contains 200 random bits and $\alpha = 75$, the peak signal to noise ratio (PSNR) is shown in Figure 5 for various embedding strength q_w. The watermark embedded version for $q_w = 75$ (PSNR=36.9 dB) is shown in Figure 6(b).

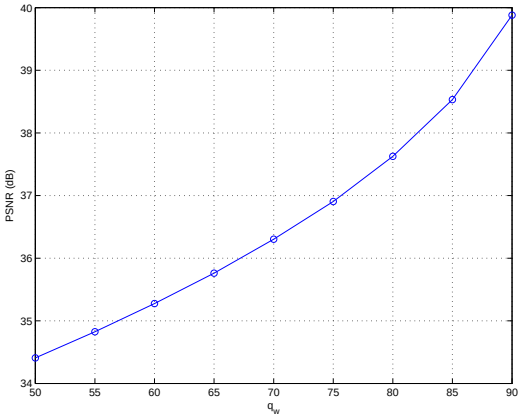


Figure 5: PSNR for different embedding strengths, $\alpha = 75$.

(a) Original (b) Embedded

Figure 6: Lena before and after watermark embedding ($q_w = 75, \alpha = 75, \text{PSNR} = 36.9$ dB).

Each image block contains on average 15 watermark bits.

In order to examine the robustness of the watermark, JPEG compression and Gaussian noise addition are applied to the embedded image. For the embedding strengths of $q_w = 55, 65, 75$, the bit error rates of the watermark after JPEG compression are plotted in Figure 7; the bit error rates for Gaussian noise are plotted in Figure 8; more experiments have been done for average filtering, gaussian filtering, and median filtering respectively (due to space constraint, plots are omitted here). The results show that, this scheme is robust against JPEG compression and Gaussian filtering; besides, it can resist weak Gaussian noise and slight filtering by average or median method.

5 SECURITY ANALYSIS

In this section, we analyze how the proposed protocol fulfills the design requirements.

Traceability. Once a pirated copy is found, the protocol enables $\mathcal{A}$ to trace the related transaction record, and $\mathcal{J}$ to identify the privacy violator.

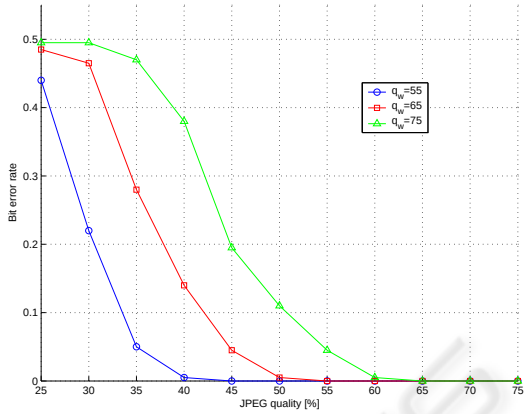


Figure 7: Robustness to JPEG compression.

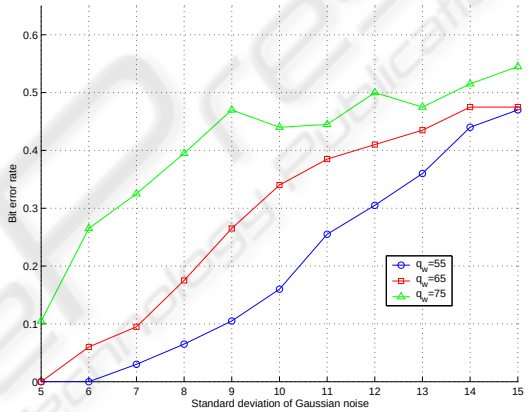


Figure 8: Robustness to Gaussian noise.

Non-framing (Buyer's Security). Since $\mathcal{A}$ only knows the encrypted content $E_{pk_{\mathcal{B}}^*}(X')$ but not $\mathcal{B}$'s watermark W_B and anonymous private key $sk_{\mathcal{B}}^*$, $\mathcal{A}$ doesn't know the watermarked content X' for $\mathcal{B}$. Therefore, the customer's rights problem is solved because $\mathcal{A}$ cannot frame $\mathcal{B}$ by distributing replicas of X' herself. The unbinding problem is solved as follows. If $\mathcal{A}$ manages to obtain a copy sold to $\mathcal{B}$ as $Y = X_0 \oplus (W_A + W_B + \phi 2^n)$, $\mathcal{A}$ can obtain W_B anyhow since she knows W_A and ϕ. Then $\mathcal{A}$ can insert the extracted W_B to another content to fabricate a copy. Even if this fabricated piracy is possible, $\mathcal{A}$ can't forge $\mathcal{B}$'s signature λ that explicitly binds $E_{pk_B^*}(W_B), pk_B^*$ to ARG, which in turn binds to a particular transaction with specifications of X. Furthermore, since $\mathcal{B}$'s anonymous key (pk_B^*, sk_B^*) is one-time, $\mathcal{A}$ cannot trick $\mathcal{B}$ by sending outdated information from previous transactions. Hence, framing attack is impossible.

Non-repudiation (Seller's Security). $\mathcal{B}$ only knows W_B but not $\mathcal{A}$'s watermark W_A nor the original content X_0. Therefore, $\mathcal{B}$ cannot remove W_B from X'. Neither

Table 2: Comparison of the plaintext space, the ciphertext space, and the expansion ratio of various probabilistic *"decisional composite residuosity assumption" (DCRA)*-based homomorphic cryptosystems.

$\mathcal{E} : \mathbb{G} \to \tilde{\mathbb{G}}$	$\mathbb{G}$	$\tilde{\mathbb{G}}$	Expansion ratio
Goldwasser-Micali (Goldwasser and Micali, 1982)	$\{0,1\}$	$\mathbb{Z}_n^*$	$lg(n)$
Benaloh (Benaloh, 1994)	$\mathbb{Z}/r\mathbb{Z}$	$(\mathbb{Z}/n\mathbb{Z})^*$	$lg(n)/lg(r)$
Naccache-Stern (Naccache and Stern, 1998)	$\mathbb{Z}/r\mathbb{Z}$	$(\mathbb{Z}/n\mathbb{Z})^*$	$lg(n)/lg(r)$
Okamoto-Uchiyama (Okamoto and Uchiyama, 1998)	$\mathbb{Z}/p\mathbb{Z}$	$\mathbb{Z}/p^2q\mathbb{Z}$	$lg(p^2q)/lg(p) > 2$
Paillier (Paillier, 1999)	$\mathbb{Z}_n$	$\mathbb{Z}_{n^2}^*$	$lg(n^2)/lg(n) = 2$
Damgård-Jurik (Jurik, 2001)	$\mathbb{Z}_{n^s}$	$\mathbb{Z}_{n^{s+1}}^*$	$(s+1)/s \leq 2$ $(s \in \mathbb{N})$

can he claim that a piracy was created by $\mathcal{A}$, because no one else can forge $\mathcal{B}$'s copy.

Conspiracy Resistance. $\mathcal{B}$ generates his own W_B and there is no third party involved in the watermark generation and insertion protocol. It enables the scheme to be resistant against conspiracy attacks.

Dispute Resolution. When a dispute occurs, $\mathcal{J}$ can recover sk_B^* from the *CA*, without $\mathcal{B}$ exposing sk_B^* and W_B. After sk_B^* is recovered, $\mathcal{J}$ can obtain W_B and he can further arbitrate the dispute.

Anonymity. $\mathcal{B}$'s anonymity is preserved because of the underlying group signature. It is computationally infeasible for an adversary, not in possession of the *CA*'s opening key *ok*, to recover the identity of $\mathcal{B}$. $\mathcal{A}$ can only know some buyer with an anonymous key pk_B^* has bought a product but not the identity.

Unlinkability. Transaction unlinkability is introduced by $\mathcal{B}$'s one-time key pair and the unlinkability property of the underlying group signature scheme.

Quality and Complexity Improvement. In the proposed scheme, only one composite watermark is required to be inserted, which reduces the computation complexity. Another obvious advantage over double watermark embedding schemes is to prevent content quality degradation and to improve robustness.

Moderate Expansion Ratio. Early anonymous fingerprinting protocols (Pfitzmann and Waidner, 1997; Pfitzmann and Sadeghi, 1999; Pfitzmann and Sadeghi, 2000) employ bit-commitment, which lead to an expansion ratio of at least 10^3 to achieve security, hence are inefficient (Kuribayashi and Tanaka, 2005). Therefore, a smaller expansion ratio, i.e., the ratio between the length of the ciphertext and the corresponding plaintext, is required. Expansion ratios of serval *DCRA*-based homomorphic cryptosystems are evaluated in Table 2. The Damgård-Jurik cryptosystem has the smallest expansion ratio of $(s+1)/s$, which closes to 1 if s is sufficiently large.

6 CONCLUSIONS

We introduced a new anonymous buyer-seller watermarking protocol based on group signatures and additive homomorphism. One improvement is to provide all the required security properties, such as revocable anonymity for the buyer, transaction unlinkability, and copyright violator traceability with the help of a trusted authority. Another improvement of our scheme is on utility. Double-watermark insertion from conventional schemes is avoided, in order to improve the product's quality, to reduce the computation complexity, and to enhance the robustness of the underlying watermark. The protocol gives the flexibility to adopt all kinds of watermarking schemes, as long as privacy homomorphism is preserved. We showed how to apply additive homomorphism, such that watermark can be embedded in the encrypted domain by adapting the quantized frequency coefficients. Furthermore, we reduce the expansion ratio from 10^3 of the conventional schemes, to 2 as the theoretical upper bound of the Damgård-Jurik cryptosystem, which is reasonable for cipher communication.

ACKNOWLEDGEMENTS

This work was supported by the Concerted Research Action (GOA) AMBioRICS 2005/11 of the Flemish Government and by the IAP Programme P6/26 BCRYPT of the Belgian State (Belgian Science Policy). The authors were supported by the Interdisciplinary institute for BroadBand Technology, Belgium.

REFERENCES

Bellare, M., Shi, H., and Zhang, C. (2005). Foundations of group signatures: the case of dynamic groups. In *Top-*

ics in Cryptology - CT-RSA 2005, LNCS 3376, pages 136–153. Springer-Verlag.

Benaloh, J. (1994). Dense probabilistic encryption. In *Proc. Selected Areas of Cryptography (SAC'94)*, pages 120–128.

Biehl, I. and Meyer, B. (1997). Protocols for collusion-secure asymmetric fingerprinting. In *Proc. 14th STACS*, LNCS 1200, pages 213–222. Springer-Verlag.

Blakley, G. R., Meadows, C., and Prudy, G. B. (1985). Fingerprinting long forgiving messages. In *Advances in Cryptology - CRYPTO 85*, LNCS 218, pages 180–189. Springer-Verlag.

Boneh, D. and Shaw, J. (1995). Collusion-secure fingerprinting for digital data. LNCS 963, pages 452–465.

Camenisch, J. (2000). Efficient anonymous fingerprinting with group signatures. In *ASIACRYPT*, LNCS 1976, pages 415–428. Springer-Verlag.

Camenisch, J. and Damgård, I. (1998). Verifiable encryption and applications to group signatures and signature sharing. In *Technical Report RS-98-32, BRICS, Department of Computer Science, University of Aarhus*.

Cox, I., Kilian, J., Leighton, T., and Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12):1673–1687.

Frattolillo, F. (2007). Watermarking protocol for web context. *IEEE Transactions on Information Forensics and Security*, 2(3):350–363.

Goi, B.-M., Phan, R. C.-W., Yang, Y., Bao, F., Deng, R. H., and Siddiqi, M. U. (2004). Cryptanalysis of two anonymous buyer-seller watermarking protocols and an improvement for true anonymity. In *Applied Cryptography and Network Security*, LNCS 2587, pages 369–382.

Goldwasser, S. and Micali, S. (1982). Probabilistic encryption and how to play mental poker hiding all partial information. In *Proceedings of the 14th Annual ACM Symposium on the Theory of Computing*, pages 365–377.

Ibrahim, I. M., El-Din, S. H. N., and Hegazy, A. F. A. (2007). An effective and secure buyer-seller watermarking protocol. In *Third International Symposium onInformation Assurance and Security, 2007. IAS 2007*, pages 21–28.

Jae-Gwi Choi, Kouichi Sakurai, J.-H. P. (2003). Does it need trusted third party? design of buyer-seller watermarking protocol without trusted third party. In *Applied Cryptography and Network Security*, LNCS 2846, pages 265–279.

Ju, H.-S., Kim, H.-J., Lee, D.-H., and Lim, J.-I. (2002). An anonymous buyer-seller watermarking protocol with anonymity control. *Information Security and Cryptology - ICISC*, pages 421–432.

Jurik, I. D. M. (2001). A generalisation, a simplification and some applications of paillier's probabilistic public-key system. In *4th International Workshop on Practice and Theory in Public-Key Cryptography*, LNCS 1992, pages 119–136. Springer-Verlag.

Kuribayashi, M. and Tanaka, H. (2005). Fingerprinting protocol for images based on additive homomorphic property. *IEEE Transactions on Image Processing*, 14(12):2129–2139.

Lei, C.-L., Yu, P.-L., Tsai, P.-L., and Chan, M.-H. (2004). An efficient and anonymous buyer-seller watermarking protocol. *IEEE Transactions on Image Processing*, 13(12):1618–1626.

Liu, K., Trappe, W., Wang, Z., Wu, M., and Zhao, H. (2005). *Multimedia Fingerprinting Forensics for Traitor Tracing*. EURASIP Book Series on Signal Processing and Communications. Hindawi Publishing Co.

Memon, N. D. and Wong, P. W. (2001). A buyer-seller watermarking protocol. *IEEE Transactions on Image Processing*, 10(4):643–649.

Naccache, D. and Stern, J. (1998). A new public-key cryptosystem based on higher residues. In *5th ACM Conference on Computer and Communications Security*, pages 59–66. ACM.

Okamoto, T. and Uchiyama, S. (1998). A new public-key cryptosystem as secure as factoring. In *Advances in Cryptology - EUROCRYPT'98*, LNCS 1403, pages 308–318. Springer-Verlag.

Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In *Advances in Cryptology - EUROCRYPT'99*, LNCS 1592, pages 223–238. Springer-Verlag.

Pfitzmann, B. and Sadeghi, A.-R. (1999). Coin-based anonymous fingerprinting. In *Advances in Cryptology - EUROCRYPT'99*, LNCS 1592, pages 150–164. Springer-Verlag.

Pfitzmann, B. and Sadeghi, A.-R. (2000). Anonymous fingerprinting with direct non-repudiation. In *Advances in Cryptology - ASIACRYPT '00*, LNCS 1976, pages 401–414. Springer-Verlag.

Pfitzmann, B. and Waidner, M. (1997). Anonymous fingerprinting. In *Advances in Cryptology - EUROCRYPT'97*, pages 88–102.

Pittzmann, B. and Schunter, M. (1996). Asymmetric fngerprinting. In *Advances in Cryptology - EUROCRYPT'96*, LNCS 1070, pages 84–95. Springer-Verlag.

Qiao, L. and Nahrstedt, K. (1998). Watermarking schemes and protocols for protecting rightful ownership and customer's rights. *Journal of Visual Communication and Image Representation*, 9(3):194 – 210.

Trappe, W., Wu, M., Wang, Z. J., and Liu, K. J. R. (2003). Anti-collusion forensics of multimedia fingerprinting using orthogonal modulation. *IEEE Transactions on Image Processing*, 51(4):1069 – 1087.

Wang, Z. J., Wu, M., Zhao, H. V., Trappe, W., and Liu, K. J. R. (2005). Anti-collusion forensics of multimedia fingerprinting using orthogonal modulation. *IEEE Transactions on Image Processing*, 14(6):804 – 821.

Zhang, J., Kou, W., and Fan, K. (2006). Secure buyer-seller watermarking protocol. In *IEE Proceedings Information Security*, volume 153, pages 15–18.