10

Recent Fingerprinting Techniques with Cryptographic Protocol

Minoru Kuribayashi
Kobe University
Japan

1. Introduction

According to the development of the Internet, multi-media contents such as music, picture, movie, etc. are treated by digital format on the network. It enables us to purchase digital contents via a net easily. However, it causes several problems such as violation of ownership and illegal distribution of the copy. Digital fingerprinting is used to trace back the illegal users, where unique ID known as digital fingerprints is embedded into digital contents before distribution Wu et al. (2004). When a suspicious copy is found, the owner can identify illegal users by extracting the fingerprint. The fingerprinting techniques of multimedia contents involve the generation of a fingerprint, the embedding operation, and the realization of traceability from redistributed copies. The research on such fingerprinting techniques is classified into two studies; secure cryptographic protocol and design of collusion resistant fingerprint.

In a cryptographic protocol, the goal is to achieve the asymmetric property between a buyer and a seller such that only the former can obtain a uniquely fingerprinted copy because of the threat of dispute. If both of the parties know the fingerprinted copy, the buyer may redistribute a pirated copy but later repudiate it by insisting that it came from the seller. An asymmetric protocol Pfitzmann & Schunter (1996) is executed by exploiting the homomorphic property of the public key cryptosystem that enables a seller to produce the ciphertext of fingerprinted copy by operating an encrypted fingerprint with encrypted contents.

Since each user purchases multimedia contents involving his own fingerprint, each copy is slightly different. A coalition of users will therefore combine their different marked copies of a same content for the purpose of removing/changing the original fingerprint. A number of works on designing fingerprints that are resistant against the collusion attack have been proposed. Many of them can be categorized into two approaches. One is to exploit the Spread Spectrum (SS) technique Cox et al. (1997); Wang et al. (2004; 2005); Zhao et al. (2005), and the other approach is to devise an exclusive code, known as collusion-secure code Boneh & Shaw (1998); Staddon et al. (2001); Tardos (2003); Trappe et al. (2003); Yacobi (2001); Zhu et al. (2005), which has traceability of colluders. Although cryptographic protocols provide the asymmetric property, the production of embedding information is based on the design of collusion-resistant fingerprint.

In this chapter, we introduce the implementation method of watermarking technique in the encrypted domain during the fingerprinting protocol. As the robustness against attacks, a transformed domain like frequency domain is generally suitable to embed watermark information into an image. In such a case, the components of the transformed domain may be represented by real values. In order to apply a public-key cryptosystem, all frequency components of an image must be quantized to integer. In the operation, a fingerprinting information is embedded to the quantized value. From the perceptual property, the changes in low frequency components stand out compared with that of the other components and hence each component is quantized adaptively by a special quantization step size. In the conventional method Kuribayashi & Tanaka (2005), for the embedding of an information bit of which value is unknown, the frequency components in the embedding positions are quantized to a special number before embedding so that the value can be changed depending on the information bit, which embedding method is based on QIM watermarking Chen & Wornel (2001). We propose the method for implementing the spread spectrum watermarking technique by carefully designing parameters for rounding operation. As the precision of the representing watermark signal is sensitive for the implementation, the parameters are scaled by multiplying a constant factor. For the characteristic of the fingerprinting protocol, frequency components and the watermark signal must be separately encrypted after quantization. In such a case, the consistency of the precision is a sensitive issue. Then, the separate rounding operation causes interference term in a deciphered data at a buyer side. Without loss of secrecy of an original content, the interference term is removed after decryption in the post-processing. The proposed approach provides a guideline for the selection of watermarking technique suitable for a multimedia forensic system.

2. Fingerprinting Protocol

One of serious threats in the fingerprinting is dispute and repudiation of a purchase. The purpose of fingerprinting protocol is to solve such threats by achieving the asymmetric property, where only a buyer knows a fingerprinted copy. If both a buyer and a seller know a fingerprinted copy, the seller cannot prove to a third party whose copy it was even if the buyer's fingerprint can be extracted. This is because a malicious seller may distribute the copy in order to frame an innocent buyer. Hence, it is desirable that only a buyer is able to obtain his own fingerprinted copy in the protocol. Such a protocol is called the asymmetric fingerprinting protocol. As in real-life market places, it is desired that electronic market places offer privacy to the customers. It should be possible to buy different articles anonymously, since purchased items can reveal a lot of behavioristic information about a buyer. The solution is the anonymous fingerprinting protocol. Thus, the fingerprinting protocol is classified into the following three classes.

Symmetric: The operation to embed a fingerprint is performed only by a seller. Therefore, he cannot convince any third party of the traitor's treachery even if he has found out the identity of a traitor in an illegal copy.

Asymmetric: Fingerprinting is an interactive protocol between a buyer and a seller. After the sale, only the buyer obtains the copy with a fingerprint. If the seller finds the fingerprinted copy somewhere, he can identify the traitor and convince a third party that the the copy is illegally distributed by the traitor.

Anonymous: A buyer can purchase a fingerprinted copy without informing his identity to a seller, but he can identify the traitor later. It also retains the asymmetric property.

In asymmetric fingerprinting, the plain value of a fingerprint should not be revealed to a seller, otherwise he can produce a fingerprinted copy by himself. Therefore an interactive protocol is performed to prevent the seller obtaining the fingerprinted copy. Such a protocol is based on public-key cryptosystems because they assure only a buyer can decrypt a ciphertext though both of them can perform the enciphering operation. In order to achieve the asymmetric fingerprinting, a homomorphic property of public-key cryptosystems is applied.

2.1 Asymmetric Property

In order to achieve an asymmetric property, a homomorphic property of public-key cryptosystems is introduced in the fingerprinting protocols Pfitzmann & Sadeghi (1999). The homomorphic property enables a seller to obtain the ciphertext of fingerprinted copy by operating an encrypted fingerprint with an encrypted original content. Since the ciphertext is computed using a buyer's encryption key, only the buyer can decrypt it; hence, only he can obtain the fingerprinted copy.

The homomorphic property of public-key cryptosystems is often applied for cryptographic protocol as operations that can be performed without revealing the plain value. If an operation on a ciphertext space results in an operation on the message space, the cryptosystem is homomorphic, and principally the former operation is multiplication and the latter is one of three operations, *"addition, multiplication, exclusive or"*, in public-key cryptosystems.

Let $E(M)$ be a ciphertext of a message M. The homomorphic property satisfies the following equation:

$$g\big(E(M_1), E(M_2)\big) = E\big(f(M_1, M_2)\big), \tag{1}$$

where $g(\cdot)$ and $f(\cdot)$ is one of the operations, *addition, multiplication, XOR,* etc., which is related to the applied cryptosystem and the embedding algorithm (Most public-key cryptosystems select multiplication for $g(\cdot)$). If M_1 is regarded as a digital content and M_2 as a fingerprint, the fingerprint can be embedded in the content without decryption by multiplying those ciphertexts. Since they are calculated using buyer's public encryption-key, the fingerprinted copy is decrypted only by the buyer, hence the asymmetric property is satisfied. The embedding operation based on the homomorphic property is basically performed for each element of fingerprint information which will be composed of bit-sequence or spread spectrum sequence, hence each element is separately embedded in its corresponding position. Thus, M_1 is not the entire content, but one of the components like the frequency elements to be fingerprinted by a watermarking technique. Note that in watermarking techniques Katzenbeisser & Petitcolas (2000) for digital images, it is advisable to embed information in the frequency components for both the robustness and perceptual quality. When the vector representation of M_1 is given by $\{m_{1,1}, m_{1,2}, m_{1,3}, \ldots\}$, the ciphertext is also represented as $E(M_1) = \{E(m_{1,1}), E(m_{1,2}), E(m_{1,3}), \ldots\}$. As the consequence, the detail of Eq.(1) is given by

$$g\big(E(m_{1,i}), E(m_{2,i})\big) = E\big(f(m_{1,i}, m_{2,i})\big),\ (i = 1, 2, 3, \ldots). \tag{2}$$

The multiplicative property of RSA scheme Rivest et al. (1978) is applied to embed a fingerprint in Memon & Wong (2001), the homomorphism of a bit commitment scheme based on the quadratic residues Brassard et al. (1988) is exploited Pfitzmann & Sadeghi (1999; 2000), and the additive homomorphic property of public-key cryptosystem such as Okamoto-Uchiyama encryption scheme Okamoto & Uchiyama (1998) and Paillier cryptosystem Paillier (1999) is utilized in Kuribayashi & Tanaka (2005). In these schemes, to convince a seller that a transmitted ciphertexts really contains his fingerprinting information, zero-knowledge interactive protocol (ZKIP) must be performed, which is easily constructed using the applied public-key cryptosystem. Such characteristic is necessary for the security reason and the anonymity of a buyer is achieved.

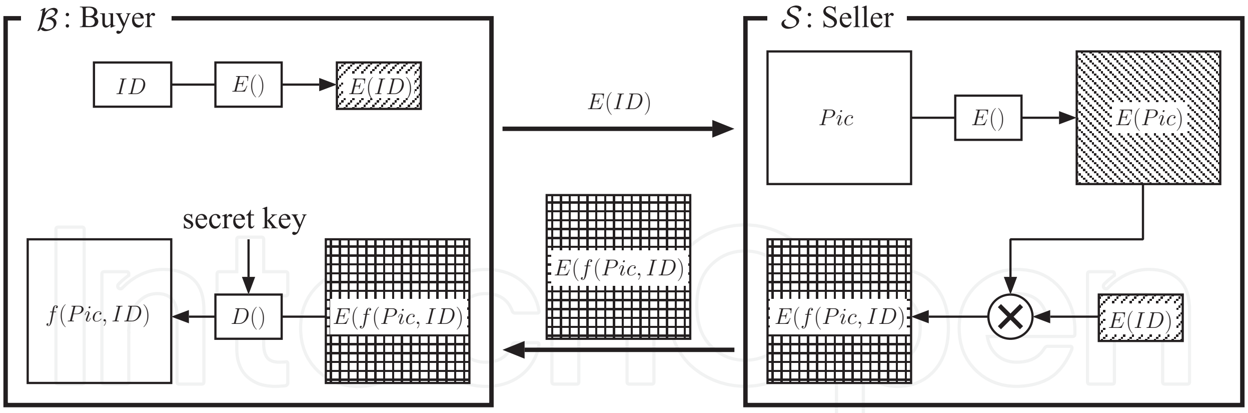

Fig. 1. The flow of the asymmetric fingerprinting protocol.

2.2 Asymmetric Fingerprinting Protocol Based on Bit Commitments

In the asymmetric fingerprinting scheme, a buyer and a seller jointly embed a fingerprint. First, the buyer encrypts a fingerprint and sends it to the seller. Then the seller verifies that the received ciphertext is made from the real fingerprint, and embeds it in his encrypted copy by multiplying those ciphertexts. Finally, the buyer receives the encrypted and fingerprinted copy and decrypts it. After the protocol, only the buyer gets the fingerprinted copy without disclosing his identity. The model of asymmetric fingerprinting protocol is described in Fig.1. A concept of an anonymous fingerprinting protocol was first presented in Pfitzmann & Waidner (1997), and the fingerprinting system composed of several protocols was presented Pfitzmann & Sadeghi (1999), which security was further improved in Pfitzmann & Sadeghi (2000). There are three parties, buyer $\mathcal{B}$, seller $\mathcal{S}$, and registration center $\mathcal{RC}$. First, $\mathcal{RC}$ generates a pair of keys, secret key and public key, and distributes the latter to all participants of the system. When $\mathcal{B}$ begins a trade to a seller $\mathcal{S}$, first $\mathcal{B}$ must register at $\mathcal{RC}$. And then $\mathcal{B}$ withdraws a digital coin which includes an identify proof $W = proof(id)$ of his identity(fingerprint), id, and its signature which can be verified using the $\mathcal{RC}$'s public key and can assure the legitimacy of the buyer. In *Fingerprinting Protocol*, $\mathcal{B}$ encrypts his fingerprint and sends to $\mathcal{S}$. Then using a zero-knowledge proof, $\mathcal{B}$ proves that the contents of the ciphertext is equivalent to that of W. After $\mathcal{S}$ is convinced the validity of the ciphertext, he encrypts his image, and multiplies the received ciphertext and the ciphertext of his image to embed the fingerprint in his image based on a homomorphic property. In order to prove that the ciphertext really includes the fingerprint without revealing the plain value, two kinds of bit commitment schemes are applied. One is based on the discrete logarithm assumption, and the other is on the quadratic residues Brassard et al. (1988) which security depends on the p-subgroup assumption and quadratic residues assumption, respectively. The commitment schemes BC_{DL} and BC_{RQ} are described as follows.

BC_{DL}**:** Let p be a large prime, and g and h be the generators. The commitment $com_{DL}(b, r)$ of a bit b is calculated using a random number r as follows.

$$com_{DL}(b, r) = g^b h^r \pmod{p} \tag{3}$$

BC_{QR}: Let p and q be large primes, and $n = pq$. The commitment $com_{QR}(b,r)$ is obtained by the following equation.

$$com_{QR}(b,r) = (-1)^b r^2 \pmod{n} \tag{4}$$

Here, it is remarkable that the committed value b of BC_{DL} is not only binary, it can take an integer of (Z/pZ). When W is calculated based on BC_{DL}, namely $W = com_{DL}(id,r) = g^{id}h^r \bmod p$, then it is difficult for a seller to embed directly the value of id using the commitment. Because of the characteristic of the commitment scheme, the recovery of the committed value is generally impossible. So instead of W, the commitment of each information bit of $id = \sum w_j 2^j$, which is calculated by $com_{QR}(w_j,r_j)$, is applied for embedding. For a certain bit $X_i \in \{0,1\}$ of digital contents, $\mathcal{S}$ computes the commitment $com_{QR}(X_i,r_i)$, and multiplies $com_{QR}(w_j,r_j)$ to it.

$$com_{QR}(X_i,r_i) \cdot com_{QR}(w_j,r_j) = (-1)^{X_i w_j}(r_i r_j)^2 \pmod{n} \tag{5}$$

It is noticed that if $X_i w_j$ is 0, the result is quadratic residue, otherwise, it is quadratic non-residue. The knowledge of two primes p and q allow $\mathcal{B}$ to compute the value $X_i w_i \bmod 2$ using the Jacobi Symbol while $\mathcal{S}$ can not determine that it is quadratic residue or not. So the security is based on the difficulty of factoring $n = pq$.
Before the above computation, $\mathcal{B}$ must certify that the values $com_{QR}(w_j,r_j)$ of the commitments are equivalent to that of W. Using BC_{DL}, $\mathcal{B}$ convinces $\mathcal{S}$ by zero-knowledge interactive protocol that the committed value of $com_{DL}(id,r)$ is equivalent to that of $com_{QR}(id,r)$. After the above protocol, only $\mathcal{B}$ can decrypt the fingerprinted copy and $\mathcal{S}$ can obtain the proof of the communication which can be used later if $\mathcal{B}$ illegally redistributes the copy.
The function $f(\cdot)$ in the homomorphic property of BC_{QR} is *exclusive or* operation. Based on the property, an encrypted fingerprint can be embedded in the encrypted copy, but the enciphering rate is extremely small because the commitment can contain only one-bit message in $\log_2 n$-bit ciphertext, where n is composed of two large primes such that the bit-length of n should be more than 1024. Therefore, the enciphering rate of this method is more than $1/1024$.

2.3 Unbinding Problem

It is also desirable for the fingerprinting protocol to solve the unbinding problem such that the relation between fingerprint information and a specific transaction performed by a buyer and a seller. In the elementary fingerprinting protocol Memon & Wong (2001), fingerprint information to be embedded is not well considered, which is merely related to user's information such as name, address, phone number, e-mail address, etc.. When a seller finds an illegal copy and detects the corresponding buyer by extracting the fingerprint, he will go to court with the collected proofs. A malicious seller, however, frames the detected buyer by embedding the obtained fingerprint into the other contents which are more expensive than the detected one what he really sold to the buyer. Therefore, once a seller obtains such a fingerprint, it is possible for him to transplant it into another much expensive contents so that he can get compensated more.
In Lei et al. (2004), a fingerprint is binded with a common agreement (ARG) by producing the signature of a trusted watermark certification authority ($\mathcal{WCA}$), and the transaction of digital contents is uniquely associated with a log file. For anonymity of buyers, a digital certification authority ($\mathcal{CA}$) is introduced in the fingerprinting protocol. A buyer $\mathcal{B}$ first randomly selects a key pair $(pk_{\mathcal{B}}, sk_{\mathcal{B}})$, where $pk_{\mathcal{B}}$ and $sk_{\mathcal{B}}$ are the public and secret keys of public-key

cryptosystem, respectively. He sends $pk_{\mathcal{B}}$, which is a pseudonym associated with $\mathcal{B}$, to $\mathcal{CA}$ in order to get an anonymous certificate $Cert_{\mathcal{CA}}(pk_{\mathcal{B}})$. When $\mathcal{B}$ makes an order to a seller $\mathcal{S}$, he checks the validity of $Cert_{\mathcal{CA}}(pk_{\mathcal{B}})$. Then $\mathcal{S}$ asks $\mathcal{WCA}$ to generate a unique watermark W for the current transaction between $\mathcal{B}$ and $\mathcal{S}$. The protocol between the buyer $\mathcal{B}$ and seller $\mathcal{S}$ is summarized below (the detail is referred to Lei et al. (2004)).

1. $\mathcal{B}$ selects one-time key pair $(pk^{\star}, sk^{\star})$ and generates its certificate $Cert_{pk_{\mathcal{B}}}(pk^{\star})$ using the public key $pk_{\mathcal{B}}$. After making a common agreement ARG, $\mathcal{B}$ calculates a digital signature $Sign_{pk^{\star}}(ARG)$ using the one-time public key $pk^{\star}$. $\mathcal{B}$ sends pk_B, $pk^{\star}$, $Cert_{\mathcal{CA}}(pk_{\mathcal{B}})$, $Cert_{pk_{\mathcal{B}}}(pk^{\star})$, ARG, and $Sign_{pk^{\star}}(ARG)$ to $\mathcal{S}$.
2. If the validity of the received items is verified, $\mathcal{S}$ generates a watermark V and embeds into contents X. The watermark is reference information to retrieve this sale record from illegally distributed copy; hence it could be omitted if the seller wants to avoid the degradation of quality. Then, $\mathcal{S}$ send $Cert_{pk_{\mathcal{B}}}(pk^{\star})$, ARG, $Sign_{pk^{\star}}(ARG)$, and $X^{(V)}$ to $\mathcal{WCA}$.
3. Upon receiving the items, $\mathcal{WCA}$ verifies the validity of the certificate and signature, and reject the transaction if any of them is invalid. Otherwise, using $X^{(V)}$ it generates a unique and robust watermark W as fingerprint information which is specific to this transaction. Then, it computes $E_{pk^{\star}}(W)$, $E_{pk_{\mathcal{WCA}}}(W)$, and $Sign_{\mathcal{WCA}}(E_{pk^{\star}}(W), pk^{\star}, Sign_{pk^{\star}}(ARG))$, and sends them back to $\mathcal{S}$.
4. When $\mathcal{S}$ receives the response, the embedding operation in encrypted domain is performed by computing

   $$E_{pk^{\star}}(X^{(W,V)}) = E_{pk^{\star}}(X^{(V)}) \oplus E_{pk^{\star}}(W), \tag{6}$$

   where $\oplus$ implies the embedding operation based on the homomorphic property. Then, $\mathcal{S}$ delivers $E_{pk^{\star}}(X^{(W,V)})$ to $\mathcal{B}$.
5. After decrypting the received $E_{pk^{\star}}(X^{(W,V)})$, $\mathcal{B}$ obtains the watermarked copy $X^{(W,V)}$.

Where $E_{pk}(\cdot)$ is an enciphering function using a public key pk. The flow of the transaction is summarized in Fig.2.

The signature $Sign_{\mathcal{WCA}}(E_{pk^{\star}}(W), pk^{\star}, Sign_{pk^{\star}}(ARG))$ explicitly binds W and ARG, which, in turn, uniquely specifies a particular digital content X, so it is impossible for $\mathcal{S}$ to transplant the watermark from an illegal copy to other contents.

3. Asymmetric Fingerprinting Protocol Based on Additive Homomorphism

The idea of the protocol Kuribayashi & Tanaka (2005) is to exploit the public-key cryptosystem with additive homomorphic property such as the Okamoto-Uchiyama encryption scheme Okamoto & Uchiyama (1998) and Paillier cryptosystem Paillier (1999) for anonymous fingerprinting.

3.1 Public-Key Cryptosystem with Additive Homomorphism

After Goldwasser-Micali's scheme Goldwasser & Micali (1984) based on quadratic residuosity, Benaloh's homomorphic encryption function, originally designed for electronic voting and relying on prime residuosity, prefigured the first attempt to exploit the plain resources of this theory. Okamoto and Uchiyama significantly extended the enciphering rate by investigating

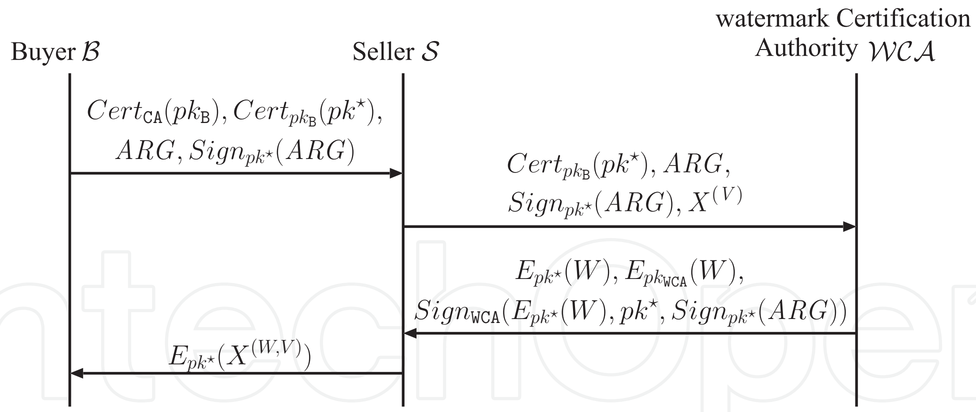
Buyer $\mathcal{B}$
Seller $\mathcal{S}$
watermark Certification Authority $\mathcal{WCA}$
$Cert_{\mathtt{CA}}(pk_{\mathtt{B}}), Cert_{pk_{\mathtt{B}}}(pk^{\star}), ARG, Sign_{pk^{\star}}(ARG)$
$Cert_{pk_{\mathtt{B}}}(pk^{\star}), ARG, Sign_{pk^{\star}}(ARG), X^{(V)}$
$E_{pk^{\star}}(W), E_{pk_{\mathtt{WCA}}}(W), Sign_{\mathtt{WCA}}(E_{pk^{\star}}(W), pk^{\star}, Sign_{pk^{\star}}(ARG))$
$E_{pk^{\star}}(X^{(W,V)})$

Fig. 2. The transaction of the fingerprinting protocol.

two different approaches: residuosity of smooth degree in $\mathbb{Z}_{pq}^*$ and residuosity of prime degree p in $\mathbb{Z}_{p^2q}^*$, respectively. Here, we review the cryptosystem and enumerate the properties of the enciphering function.

Let p and q be two large primes ($|p| = |q| = \ell_p$ bits) and $N = p^2q$. Choose $g \in_R (\mathbb{Z}/N\mathbb{Z})$ randomly such that the order of $g_p = g^{p-1} \bmod p^2$ is p, where $g.c.d.(p, q-1) = 1$ and $g.c.d.(q, p-1) = 1$. Let $h = g^N \bmod N$. Here a public key pk is (N, g, h, ℓ_p) and a secret key sk is (p, q). The cryptosystem, based on the exponentiation mod$N$, is constructed as follows.

Encryption: Let m $(0 < m < 2^{\ell_p - 1})$ be a plaintext. Selecting a random number $r \in_R (\mathbb{Z}/N\mathbb{Z})$, a ciphertext is given by

$$C = g^m h^r \pmod{N}. \tag{7}$$

Decryption: Calculate first $C_p = C^{p-1} \bmod p^2$ and then

$$m = \frac{L(C_p)}{L(g_p)} \pmod{p}, \tag{8}$$

where

$$L(x) = \frac{x-1}{p}. \tag{9}$$

We denote the encryption function $E_{pk}(m, r)$ and decryption function $D_{sk}(C)$. Three important properties of the scheme are given by the following P1, P2 and P3.

P1. It has an additive homomorphic property : if $m_1 + m_2 < p$,

$$E_{pk}(m_1, r_1) \cdot E_{pk}(m_2, r_2) = E_{pk}(m_1 + m_2, r_1 + r_2) \pmod{N}. \tag{10}$$

P2. It is semantically secure if the following assumption, *i.e.* p-subgroup assumption, is true: $E_{pk}(0, r) = h^r \bmod N$ and $E_{pk}(1, r') = gh^{r'} \bmod N$ is computationally indistinguishable, where r and r' are uniformly and independently selected from $\in_R (\mathbb{Z}/N\mathbb{Z})$.

P3. Anyone can change a ciphertext, $C = E_{pk}(m, r)$, into another ciphertext, $C' = Ch^{r'} \bmod N$, while preserving the plaintext of C (*i.e.*, $C' = E_{pk}(m, r'')$), and the relationship between C and C' can be concealed.

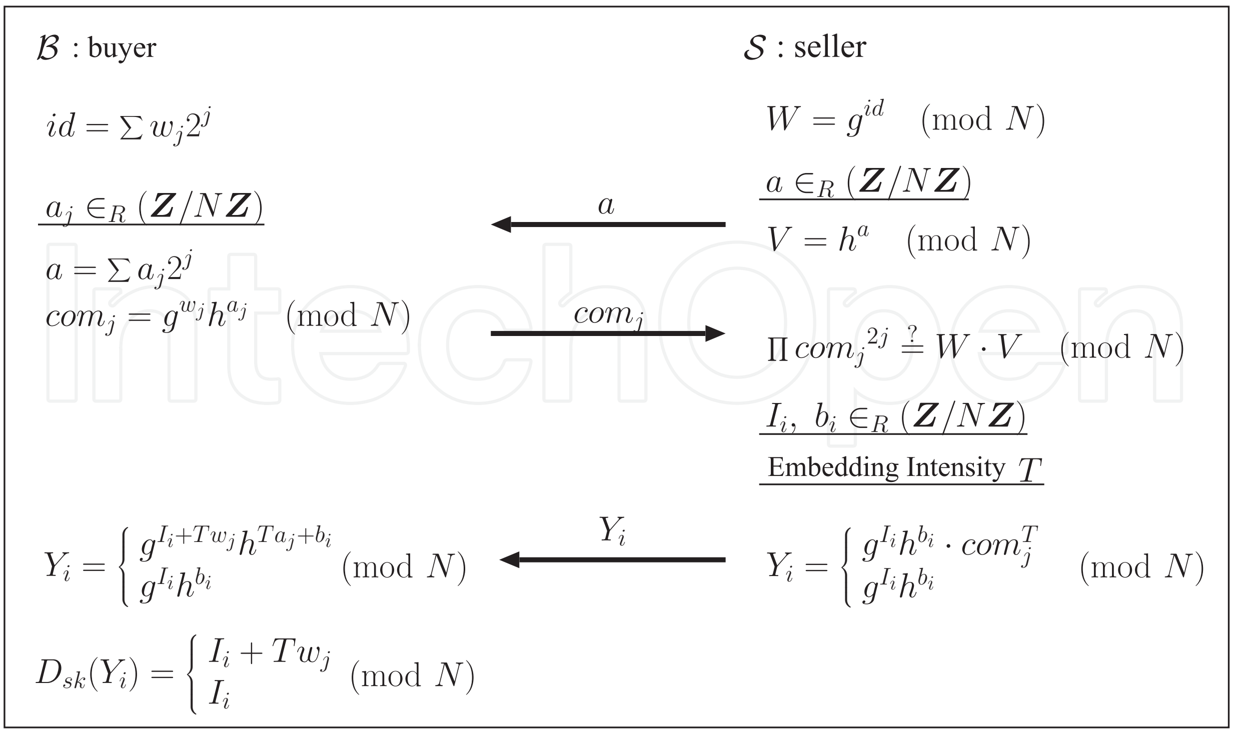
$\mathcal{B}$: buyer
$\mathcal{S}$: seller
$id = \sum w_j 2^j$
$W = g^{id} \pmod N$
$a \in_R (\boldsymbol{Z}/N\boldsymbol{Z})$
$a_j \in_R (\boldsymbol{Z}/N\boldsymbol{Z})$
a
$V = h^a \pmod N$
$a = \sum a_j 2^j$
$com_j = g^{w_j} h^{a_j} \pmod N$
com_j
$\Pi\, com_j{}^{2j} \overset{?}{=} W \cdot V \pmod N$
$I_i,\ b_i \in_R (\boldsymbol{Z}/N\boldsymbol{Z})$
Embedding Intensity T
Y_i
$Y_i = \begin{cases} g^{I_i+Tw_j} h^{Ta_j+b_i} \\ g^{I_i} h^{b_i} \end{cases} \pmod N$
$Y_i = \begin{cases} g^{I_i} h^{b_i} \cdot com_j^T \\ g^{I_i} h^{b_i} \end{cases} \pmod N$
$D_{sk}(Y_i) = \begin{cases} I_i + Tw_j \\ I_i \end{cases} \pmod N$

Fig. 3. Fingerprinting protocol based on additive homomorphism.

Although the enciphering rate of Paillier cryptosystem Paillier (1999), which has the similar structure to Okamoto-Uchiyama encryption scheme, is higher, it requires more computations. So the selection of the scheme is dependent on the applied system. For convenience, the cryptosystem in the protocol is represented by Okamoto-Uchiyama encryption scheme; the approach can be easily translated to the Paillier cryptosystem, the readers are recommended to check the original paper Paillier (1999).

3.2 Main Protocol

The fingerprinting protocol is executed between a buyer $\mathcal{B}$ and a seller $\mathcal{S}$. $\mathcal{B}$ commits his identity(fingerprint), $id = \sum w_j 2^j$ $(0 \le j \le \ell - 1)$ to $\mathcal{S}$ the enciphered form, com_j, where the values of w_j are binary. Then, $\mathcal{S}$ encrypts his image X_i $(0 \le i \le L)$ and multiplies it to the received com_j. We assume that $\mathcal{B}$ has already registered at a center $\mathcal{RC}$, and sent $\mathcal{S}$ the coin which includes a fingerprint and its signature. For simplicity, $W = g^{id} \bmod N$ is regarded as a commitment of id. Under the assumption, the fingerprinting protocol is given as follows (indicated in Fig.3).

[*Fingerprinting Protocol*]

Step 1. $\mathcal{S}$ generates a random number $a(2^\ell < a < N)$ and sends it to $\mathcal{B}$.

Step 2. $\mathcal{B}$ decomposes a into ℓ random numbers $a_j \in_R (\mathrm{Z}/N\mathrm{Z})$ to satisfy the following equation.

$$a = \sum_{j=0}^{\ell-1} a_j 2^j \tag{11}$$

Where the values of a_1 to $a_{\ell-1}$ are selected randomly under the condition,

$$\sum_{j=1}^{\ell-1} a_j 2^j < a, \tag{12}$$

and a_0 is calculated as follows.

$$a_0 = a - \sum_{j=1}^{\ell-1} a_j 2^j \tag{13}$$

A bit commitment of each w_j is calculated as

$$\begin{aligned} com_j &= g^{w_j} h^{a_j} \pmod{N}, & (14)\\ &= E_{pk}(w_j, a_j) \pmod{N}, & (15) \end{aligned}$$

and sent to $\mathcal{S}$.

Step 3. To verify the commitment, $\mathcal{S}$ calculates

$$V = h^a \pmod{N}, \tag{16}$$

and makes sure that the following equation can be satisfied.

$$\prod_j com_j^{2^j} \stackrel{?}{=} W \cdot V \pmod{N} \tag{17}$$

Step 4. $\mathcal{S}$ generates L random numbers $b_i \in_R (\mathbb{Z}/N\mathbb{Z})$ and embedding intensity T of even number. Then, in order to get the encrypted and fingerprinted image, $\mathcal{S}$ calculates

$$Y_i = \begin{cases} g^{X_i} h^{b_i} \cdot com_j^T \pmod{N} & \text{marking position} \\ g^{X_i} h^{b_i} \pmod{N} & \text{elsewhere} \end{cases} \tag{18}$$

and sends it to $\mathcal{B}$

Step 5. Since the received Y_i is rewritten as

$$Y_i = \begin{cases} g^{(X_i+Tw_j)} h^{Ta_j+b_i} \pmod{N} & \text{marking position} \\ g^{X_i} h^{b_i} \pmod{N} & \text{elsewhere,} \end{cases} \tag{19}$$

$\mathcal{B}$ can decrypt Y_i to get the plaintext.

$$D_{sk}(Y_i) = \begin{cases} X_i + Tw_j \pmod{p} & \text{marking position} \\ X_i \pmod{p} & \text{elsewhere} \end{cases} \tag{20}$$

On the deciphered message, if $w_j = 1$, then X_i has been increased, and if $w_j = 0$, then nothing has done to X_i.

Remark 1: If we regard w_j as a message and a_j as a random number, then com_j is represented by $E_{pk}(w_j, a_j)$ and com_j^T by $E_{pk}(Tw_j, Ta_j)$ because

$$\begin{aligned} com_j^T &= (g^{w_j} h^{a_j})^T \pmod N \\ &= g^{Tw_j} h^{Ta_j} \pmod N \\ &= E_{pk}(Tw_j, Ta_j). \end{aligned} \tag{21}$$

In many watermarking schemes, the embedding procedure is performed by an addition of watermark signal, namely a watermark is added to or subtracted from pixel values or frequency components with a certain intensity. Therefore, the additive homomorphism is suitable for such watermark schemes. In Eq.(18), $g^{X_i} h^{b_i} = E_{pk}(X_i, b_i)$ is regarded as $\mathcal{S}$'s enciphered image, and then from the property P1 Y_i at the marking position is rewritten as

$$\begin{aligned} Y_i &= E_{pk}(X_i, b_i) \cdot E_{pk}(Tw_j, Ta_j) \\ &= E_{pk}(X_i + Tw_j, Ta_j + b_i) \end{aligned} \tag{22}$$

If $\mathcal{S}$ uses X_i as a pixel value directly, the above operation can be applied easily. Considering about the robustness against attack such as lossy compression and filtering operation, etc., the transformed domain is generally more resilience for such attacks.

In the fingerprinting protocol $\mathcal{B}$ may be able to forge his identity as he has not proved that the values of w_j $(0 \le j \le \ell - 1)$ are binary. Even if they are not binary, Eq.(17) can be satisfied choosing them suitably. Then a malicious buyer may try to find the embedding position by setting the values adaptively. To solve the problem, a zero-knowledge interactive protocol has been introduced to prove that a commitment contains binary value, the procedure, called *binary proof*, is clearly described in Kuribayashi & Tanaka (2005).

3.3 Modified Fingerprinting Protocol

We consider the size of the message being encrypted, where the bit length of a message is revealed as the public key ℓ_p of Okamoto-Uchiyama encryption scheme. Since X_i and T are much smaller than $2^{\ell_p - 1} (< p)$ and the ciphertext is three times as large as p, the enciphering rate is still low. To exploit the message space effectively, the size of message to be encrypted should be modified as large as $2^{\ell_p - 1}$.

Let m_i be

$$m_i = \begin{cases} X_i + Tw_j & \textit{markingposition} \\ X_i & \textit{elsewhere}, \end{cases} \tag{23}$$

and ℓ_m be the maximum bit-length of m_i. Since ℓ_m is much smaller than ℓ_p, the message can be replaced by

$$M_{i'} = \sum_{t=0}^{\gamma-1} m_{i'\gamma+t} 2^{\ell_m t}, \qquad 0 \le i' \le L/\gamma - 1, \tag{24}$$

where

$$\gamma = \left\lceil \frac{\ell_p}{\ell_m} \right\rceil. \tag{25}$$

It is illustrated in Fig.4. If the ciphertext of the message $M_{i'}$ is calculated by $\mathcal{S}$ using com_j and X_i in the fingerprinting protocol, the enciphering rate becomes at most $1/3$ in theory.

In order to perform the above operations, the fingerprinting protocol of Step 4 and Step 5 presented in the fingerprinting protocol is changed as follows.

$$M_i' = \overbrace{\underbrace{\boxed{m_{i'\gamma}}}_{\ell_m\text{ bits}}\underbrace{\boxed{m_{i'\gamma+1}}}_{\ell_m\text{ bits}}\underbrace{\boxed{m_{i'\gamma+2}}}_{\ell_m\text{ bits}}\boxed{\quad\bullet\;\bullet\;\bullet\quad}\underbrace{\boxed{m_{(i'+1)\gamma-2}}}_{\ell_m\text{ bits}}\underbrace{\boxed{m_{(i'+1)\gamma-1}}}_{\ell_m\text{ bits}}}^{\ell_p\text{ bits}}$$

Fig. 4. Composition of the message $M_{i'}$.

[*Modified Fingerprinting Protocol*]

Step 4. In order to get the encrypted and fingerprinted image y_i, $\mathcal{S}$ calculates

$$y_i = \begin{cases} g^{X_i} \cdot com_j^T \pmod N & \text{marking position} \\ g^{X_i} \pmod N & \text{elsewhere.} \end{cases} \tag{26}$$

To synthesize some y_i in one ciphertext $Y_{i'}$, the following operation is performed using a random number $b_{i'} \in_R (\mathrm{Z}/N\mathrm{Z})$.

$$Y_{i'} = \Big(\prod_t (y_{i'\gamma+t})^{2^{\ell_m t}}\Big) \cdot h^{b_{i'}} \pmod N \tag{27}$$

Step 5. $\mathcal{B}$ decrypts the received $Y_{i'}$ to obtain $M_{i'}$. Since he knows the bit-length ℓ_m of m_i, he can decompose $M_{i'}$ into the pieces, and finally he can get the fingerprinted image.

Remark 3: From Eqs.(23)-(26) and the property P3, Eq.(27) is expressed by

$$\begin{aligned} Y_{i'} &= \Big(\prod_t g^{m_{i'\gamma+t}2^{\ell_m t}}\Big) \cdot h^r \pmod N \\ &= g^{\sum m_{i'\gamma+t}2^{\ell_m t}} h^r \pmod N \\ &= g^{M_{i'}} h^r \pmod N \\ &= E_{pk}(M_{i'}, r). \end{aligned} \tag{28}$$

If the Okamoto-Uchiyama encryption scheme is secure and the bit-length of $M_{i'}$ is less than ℓ_p, $\mathcal{B}$ can decrypt $Y_{i'} = E(M_{i'}, r)$. Here, in Eqs.(27) and (28) several pieces $m_{i'\gamma+t}$ of fingerprinted image that compose $M_{i'}$ are encrypted in one ciphertext $E(M_{i'}, r)$, though each piece is encrypted in the original scheme. Therefore, $M_{i'}$ should retain a special data structure described by Eq.(24). If $\mathcal{S}$ changes the data structure, $\mathcal{B}$ can not decompose it into the correct pieces $m_{i'\gamma+t}$, and then he can claim the fact. Hence, with the knowledge of data structure $\mathcal{B}$ can decompose the decrypted message $M_{i'}$ into $m_{i'\gamma+t}$, and finally get the fingerprinted image. Furthermore, as $M_{i'}$ is simply produced by composing several pieces of $m_{i'\gamma+t}$, $\mathcal{B}$ can not derive any information about original image from the decrypted message.

Assume that the size of fingerprint is ℓ bits, and the fingerprint is embedded in the frequency components of an image where the number of components is L and each component is expressed by $\ell_{\overline{m}}$ bits. Then the total amount of plain data of digital contents is $\ell_{\overline{m}}L$. In Pfitzmann & Sadeghi (1999) and Pfitzmann & Sadeghi (2000), the modulus n is a composite of two large primes. Since only one bit is encrypted when bit commitment schemes are used, each bit of the frequency components must be encrypted, thus the total amount of encrypted data is $\ell_{\overline{m}}L\log_2 n$ bits. On the other hand, the modulus of the fingerprinting protocol with additive homomorphism is $N(= p^2q,\ 3\ell_p$ bits). In the original scheme, the amount of encrypted

conventional	original	modified
$1/3\ell_p$	$\ell_{\overline{m}}/3\ell_p$	$1/3$

Table 1. Enciphering rate.

data is $L\log_2 N(=3\ell_p L)$ bits as each component is encrypted. In the modified scheme, it is $(L\log_2 N)/\gamma\,(\simeq 3\ell_{\overline{m}}L)$ bits, because from Eq.(25) there are at most L/γ messages $M_{i'}$ to be encrypted, since $\ell_m \simeq \ell_{\overline{m}}$. Here, if $\log_2 n \simeq \log_2 N = 3\ell_p$, the enciphering rates are indicated in Table 1. Since the enciphering rate of Paillier cryptosystem is $1/2$, the protocol can achieve the rate if the cryptosystem is applied instead of Okamoto-Uchiyama encryption scheme.

4. Collusion Resilience

In a fingerprinting scheme, each watermarked copy is slightly different, hence, malicious users will collect their copies in order to remove/alter the watermark. For an improperly designed fingerprint, it is possible to gather a small coalition of colluders and sufficiently attenuate each of colluders' fingerprint to produce a pirated copy with no detectable traces. Thus, it is important to model and analyze collusion, and to design fingerprints that can resist the collusion attack.

There are several types of collusion attacks that may be used against fingerprinting system. One method is to average fingerprinted copies, which is an example of the linear collusion attack. Another collusion attack involves users cutting out portions of each fingerprinted copy and pasting them together to form a pirated copy. Other attacks may employ nonlinear operations, such as taking the maximum or median of signal values of individual copies. As the countermeasure of collusion attack, a number of works on designing fingerprints have been proposed. One approach generates mutually independent sequences, *e.g.* spread spectrum sequence, for assigning users as their fingerprints, the other approach encodes fingerprint information considering the distances among fingerprint codes.

On the former approach, spread spectrum sequences which follow a normal distribution are assigned to users as fingerprints. The origin of the spread spectrum watermarking scheme is Cox's method Cox et al. (1997) that embeds the sequence into frequency components of digital image and detects it using a correlator. Since normally distributed values allow the theoretical and statistical analysis of the method, modeling of a variety of attacks have been studied. Studies in Zhao et al. (2005) have shown that a number of nonlinear collusions such as interleaving attack can be well approximated by averaging collusion plus additive noise. So far, many variants of the spread spectrum watermarking scheme are based on the Cox's method.

Let W be a watermark signal composed of ℓ elements $w_i \in N(0,1), (0 \le i < \ell)$ and each of them is embedded into selected DCT coefficient $X_i, (0 \le i < \ell)$ based on the following equation,

$$X_i^W = X_i(1+\alpha w_i), \tag{29}$$

where $N(0,1)$ is a normal distribution with mean 0 and variance 1, and α is an embedding strength. At the detector side, we determine which SS sequence is present in a test image by evaluating the similarity of sequences. From the suspicious copy, a sequence $\tilde{W}$ is detected by calculating the difference of the original image, and its similarity with W is obtained as follows.

$$\mathrm{sim}(W, \tilde{W}) = \frac{W \cdot \tilde{W}}{\sqrt{\tilde{W} \cdot \tilde{W}}}, \tag{30}$$

If the similarity value exceeds a threshold, the embedded sequence is regarded as W.

At the detection, DCT coefficients of test image are subtracted from those of original image, and then the correlations with every candidates of watermark signal are computed. Thus, non-blind and informed watermarking scheme can be applied. In fingerprinting techniques, the original content may be available at a detection because a seller is assumed as the author, or a sales agent who knows it. A simple, yet effective collusion attack is to average some variants of copy because when c copies are averaged, the similarity value calculated by Eq.(30) results in shrinking by a factor of c, which will be roughly $\sqrt{\ell}/c$ Cox et al. (1997). Even in this case, we can detect the embedded watermark and identify the colluders by using an appropriately designed threshold.

Chen et al. Chen & Wornel (2001) showed that additive spread spectrum watermarking, in general, not good choices for embedding a bit-sequence, and, as an alternative, they introduced a new class of embedding strategies, which is referred to as "quantization index modulation (QIM)". In the study, they presented that dither modulation is a practical implementation of QIM that exhibits many of the attractive performance properties of QIM. The convenient structure of dither modulation, which is easily combined with error-correction coding, allows the system designer to achieve different rate distortion-robustness trade-offs by tuning parameters such as the quantization step size. It is also suitable for fingerprinting system by encoding fingerprint information by collusion-secure code. Thus, the combination of the QIM watermarking and collusion-secure code can provide a good fingerprinting system.

Aiming at the extraction of a fingerprint bit-sequence, the QIM watermarking is implemented in Kuribayashi & Tanaka (2005) and its variants are employed in Prins et al. (2007). In Swaminathan et al. (2006), the capability of the QIM based fingerprinting system is investigated, and the results show that one variant, which is called the spread transform dither modulation (STDM), retains an advantage under blind detection. Under non-blind detection, which is a reasonable assumption in fingerprinting system, there is still a performance gap with the spread spectrum method. It is noted that, in Yacobi (2001), the traceability is further improved by combining a spread spectrum embedding like Cox's method.

Assume that the bit-length of the message space is ℓ_M and that of each watermarked frequency components is ℓ_m. Generally, ℓ_M is much larger than ℓ_m. In order to exploit the message space effectively, dozens of watermarked frequency components are packed in one message in Kuribayashi & Tanaka (2005), hence, the enciphering rate is almost equivalent to that of an applied cryptosystem by suitably designing the message space of a ciphertext. From the viewpoint of enciphering rate, the modification of QIM method implemented in Prins et al. (2007) is not a good choice, and the improvement of the robustness against attacks is still inferior to the spread spectrum method. The adaption of fingerprinting code further restricts the scalability of the QIM based fingerprinting system because of the long code-length.

5. How to Implement Spread Spectrum Watermarking on Encrypted Domain

Despite the simple structure of the QIM watermarking, the exploitation of fingerprinting code prevents the usability for various kinds of digital contents. We note that one major drawback of the conventional methods Kuribayashi & Tanaka (2005) Prins et al. (2007) is the long code-length of the fingerprinting code. Alternatively, the spread spectrum watermarking technique Cox et al. (1997) is implemented on the fingerprinting protocol based on the homomorphic property of public-key cryptosystem in this section. Hereafter, for simplicity, the embedding of the reference information V, which is introduced in Lei et al. (2004), and a random number used for the encryption are omitted in the protocol.

The embedding operation in Eq.(29) can be easily performed using the additive homomorphic property of public-key cryptosystems such as Okamoto-Uchiyama encryption scheme Okamoto & Uchiyama (1998) and Paillier cryptosystem Paillier (1999). Remember that Eq.(22) is composed of two operations; multiplication and addition for $g(\cdot)$ and $f(\cdot)$, respectively. Since the multiplication is realized by the iteration of addition, the embedding operation is represented by the multiplication and exponentiation. Suppose that an original image is composed of L pixels and is represented by the DCT selected coefficients $X_i, (0 \leq i < \ell)$ and the remain ones $X_i, (\ell \leq i < L)$, and a watermark signal is represented by $w_i, (0 \leq i < \ell)$. Then, the embedding operation of Eq.(29) is executed in the encrypted domain as follows.

$$E_{pk}\big(X_i(1+\alpha w_i)\big) = E_{pk}(X_i) \cdot E_{pk}(w_i)^{\alpha X_i} \tag{31}$$

The above operation can be directly applied for the operation $\oplus$ in Eq.(6). Here, it is noticed that a watermark signal and DCT coefficients are generally represented by real value and they must be rounded to integer before the encryption. If such parameters are directly rounded to the nearest integers, it may result in the loss of information. Hence, they should be scaled before rounding-off. In addition, a negative number should be avoided considering the property of a cryptosystem because it is represented by much longer bit-sequence under the finite field of applied cryptosystem, which affects the other packed ones described in Eq.(27). Hence, a rounding operation that maps real value into positive integer is required.

At first, we show the operation concerning to a watermark signal $W = \{w_0, w_1, w_2, \ldots, w_{\ell-1}\}$. Since the ciphertext of W is computed by a watermark certification authority $\mathcal{WCA}$, the enciphering operation is performed previously sent to a seller $\mathcal{S}$. A constant value p_w is added to each element of watermark signal $w_i, (0 \leq i < \ell)$ to make the value positive. Then, it is scaled by a factor of s_w in order to keep the degree of precision, and it is quantized to $\overline{w}_i$. Such operations are formalized by the following one equation;

$$\overline{w}_i = int\big(s_w(w_i + p_w)\big),\ 0 \leq i < \ell \tag{32}$$

where $int(a)$ outputs the nearest integer from a real value a. After the operation, $\mathcal{WCA}$ encrypts $\overline{W} = \{\overline{w}_0, \overline{w}_1, \overline{w}_2, \ldots, \overline{w}_{\ell-1}\}$ using a public key pk, and the ciphertexts $E_{pk}(\overline{W}) = \{E_{pk}(\overline{w}_0), E_{pk}(\overline{w}_1), E_{pk}(\overline{w}_2), \ldots, E_{pk}(\overline{w}_{\ell-1})\}$, p_w, and s_w are sent to $\mathcal{S}$. It is noted that $E_{pk}(\overline{W})$ corresponds to $E_{pk^\star}(W)$ in Fig.2, and the corresponding ciphertext of $E_{pk_{\mathcal{WCA}}}(\overline{W})$ is also sent to $\mathcal{S}$.

Next, $\mathcal{S}$ performs the rounding operation to DCT coefficients $X_i, (0 \leq i < \ell)$ as follows. A constant value p_x is added to each DCT coefficient, and then scaled by $s_w s_x$. By quantizing it, the rounded DCT coefficient $\overline{X}_i$ is obtained.

$$\overline{X}_i = int\big(s_w s_x(X_i + p_x)\big),\ 0 \leq i < \ell \tag{33}$$

For the control of rounding operation of each DCT coefficient, the watermark strength α is modified to $\overline{\alpha}_i$;

$$\overline{\alpha}_i = int\big(s_x \alpha |X_i|\big),\ 0 \leq i < \ell \tag{34}$$

Using the above items, $\mathcal{S}$ embeds $\overline{w}_i$ into $\overline{X}_i$ for $0 \leq i < \ell$ based on the additive homomorphic property of public cryptosystem as follows.

$$E_{pk}(\overline{X}_i) \cdot E_{pk}(\overline{w}_i)^{\overline{\alpha}_i} = E_{pk}(\overline{X}_i + \overline{\alpha}_i \overline{w}_i) \tag{35}$$

Since the plain value of the ciphertext $E_{pk}(\overline{X}_i + \overline{\alpha}_i\overline{w}_i)$ is

$$\begin{aligned} \overline{X}_i + \overline{\alpha}_i\overline{w}_i &= s_w s_x(X_i + p_x) + s_x\alpha|X_i|s_w(w_i + p_w), & (36)\\ &= s_w s_x\big((X_i + \alpha w_i|X_i|) + (p_x + \alpha|X_i|p_w)\big), & (37)\end{aligned}$$

the scaling factor $s = s_w s_x$ and the adjustment factor $p = p_x + \alpha|X_i|p_w$ are necessary to calculate the actual watermarked DCT coefficients $X_i + \alpha w_i|X_i|$. Therefore, these two parameters s and p are sent to $\mathcal{B}$ as well as $E_{pk}(\overline{X}_i + \overline{\alpha}_i\overline{w}_i)$. It is noticed that the remained DCT coefficients $X_i, (\ell \leq i < L)$ should be sent to $\mathcal{B}$. In order to keep the secrecy of the embedding position, they must be encrypted before delivery. Without loss of generality, the rounding operation for those coefficients are given by

$$\overline{X}_i = int\big(s_x s_w(X_i + p_x + \alpha|X_i|p_w)\big),\ \ell \leq i < L, \tag{38}$$

and the ciphertexts $E_{pk}(\overline{X}_i)$ are sent with $E_{pk}(\overline{X}_i + \overline{\alpha}_i\overline{w}_i)$ to $\mathcal{B}$. Namely, the ciphertexts of a watermarked image $E_{pk}(\overline{X}^W)$, which is corresponding to $E_{pk^\star}(X^{(W,V)})$ in Fig.2, is composed of those ones.

$$E_{pk}(\overline{X}^W) = \begin{cases} E_{pk}(\overline{X}_i + \overline{\alpha}_i\overline{w}_i) & 0 \leq i < \ell \\ E_{pk}(\overline{X}_i) & \ell \leq i < L \end{cases} \tag{39}$$

After the decryption of the received ciphertexts $E_{pk}(\overline{X}^W)$, $\mathcal{B}$ divides the results by a factor of s, and then subtracts p as the post-processing operation. At the embedding position, the ciphertexts are $E_{pk}(\overline{X}_i + \overline{\alpha}_i\overline{w}_i)$ and the post-processing operation outputs the fingerprinted coefficients $X_i + \alpha w_i|X_i|$ as follows;

$$\frac{D_{sk}\big(E_{pk}(\overline{X}_i + \overline{\alpha}_i\overline{w}_i)\big)}{s} - p = X_i + \alpha w_i|X_i|,\ 0 \leq i < \ell, \tag{40}$$

where $D_{sk}(\cdot)$ is a deciphering function using a secret key sk. At the other position, the ciphertexts are $E_{pk}(\overline{X}_i)$ and $\mathcal{B}$ obtains X_i after the post-processing operation.

$$\frac{D_{sk}\big(E_{pk}(\overline{X}_i)\big)}{s} - p = X_i,\ \ell \leq i < L. \tag{41}$$

It is remarkable that the embedding position is kept secret from $\mathcal{B}$, the classification of the above operations is difficult. The diagram of the interactive protocol is shown in Fig.5.

In Eq.(22), the watermarked coefficient X_i^W is composed of two terms; X_i and $\alpha w_i X_i$. Since w_i is encrypted at the center $\mathcal{WCA}$ prior to the embedding operation at $\mathcal{S}$, X_i and w_i are rounded separately. Considering the post-processing at $\mathcal{B}$, the scaling factors s_w, s_x, and the compensation factor p should be constant. Here, we assume that a constant value is uniformly added to real values which are w_i and X_i to make it positive. Then, $\mathcal{B}$ must subtract the interference term related to both X_i and w_i, which requires additional communication costs. If the adjustment factor p is varied with respect to X_i, the amount of information to be sent to $\mathcal{B}$ from $\mathcal{S}$ becomes very large. In order to avoid it, we set p a constant value by controlling the value p_x. Even if p and α is known, to obtain X_i is still informationally difficult because of three unknown parameters p_x, p_w, and X_i for a given one equation $p = p_x + \alpha|X_i|p_w$. As the consequence, the secrecy of the original DCT coefficients is assured.

Notice that if the size of scaling factors s_w and s_x is increased, the proposed scheme can simulate the original Cox's method more precisely. From the viewpoint of enciphering rate, however, these factors should be small. Referring to the modified fingerprinting protocol, the

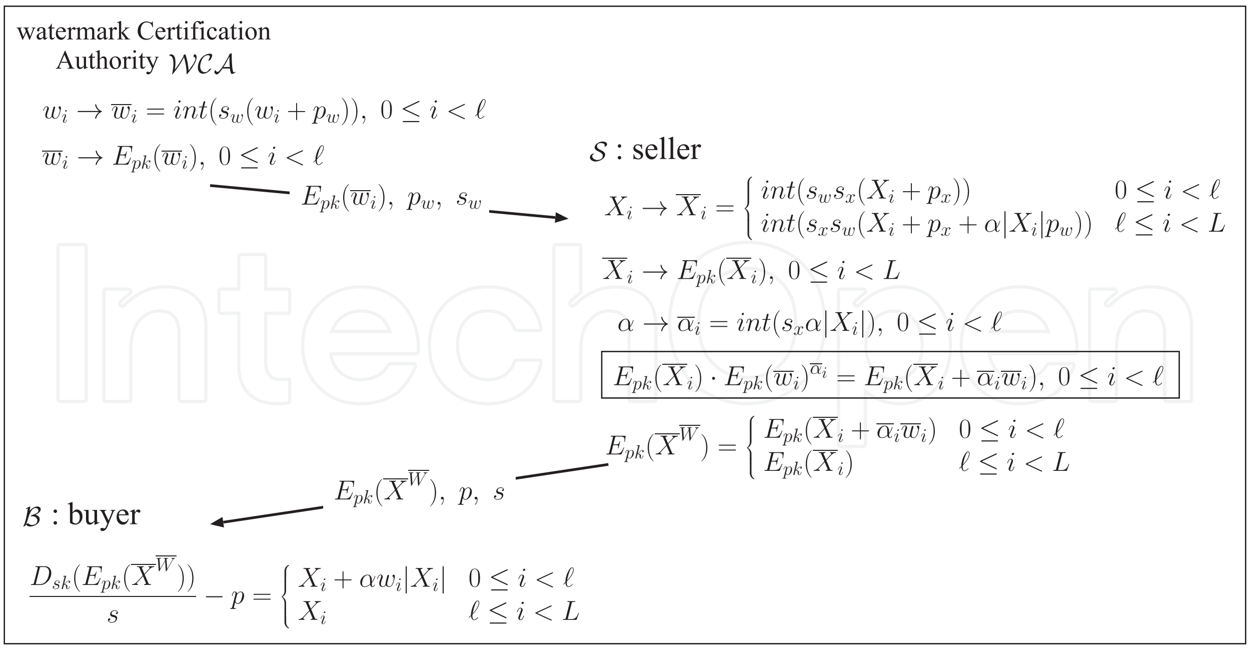
watermark Certification Authority $\mathcal{WCA}$
$w_i \to \overline{w}_i = int(s_w(w_i + p_w)),\ 0 \le i < \ell$
$\overline{w}_i \to E_{pk}(\overline{w}_i),\ 0 \le i < \ell$
$E_{pk}(\overline{w}_i),\ p_w,\ s_w$
$\mathcal{S}$: seller
$X_i \to \overline{X}_i = \begin{cases} int(s_w s_x(X_i + p_x)) & 0 \le i < \ell \\ int(s_x s_w(X_i + p_x + \alpha|X_i|p_w)) & \ell \le i < L \end{cases}$
$\overline{X}_i \to E_{pk}(\overline{X}_i),\ 0 \le i < L$
$\alpha \to \overline{\alpha}_i = int(s_x \alpha |X_i|),\ 0 \le i < \ell$
$\boxed{E_{pk}(\overline{X}_i) \cdot E_{pk}(\overline{w}_i)^{\overline{\alpha}_i} = E_{pk}(\overline{X}_i + \overline{\alpha}_i \overline{w}_i),\ 0 \le i < \ell}$
$E_{pk}(\overline{X}^{\overline{W}}) = \begin{cases} E_{pk}(\overline{X}_i + \overline{\alpha}_i \overline{w}_i) & 0 \le i < \ell \\ E_{pk}(\overline{X}_i) & \ell \le i < L \end{cases}$
$E_{pk}(\overline{X}^{\overline{W}}),\ p,\ s$
$\mathcal{B}$: buyer
$\frac{D_{sk}(E_{pk}(\overline{X}^{\overline{W}}))}{s} - p = \begin{cases} X_i + \alpha w_i |X_i| & 0 \le i < \ell \\ X_i & \ell \le i < L \end{cases}$

Fig. 5. The procedure of fingerprinting protocol to embed the spread spectrum watermark.

bit-length of a watermarked coefficient $\overline{X}_i^{\overline{W}} = \overline{X}_i + \overline{\alpha}_i \overline{w}_i$, which is represented by a constant bit-length ℓ_x, is much smaller than that of message space in cryptosystems such as Okamoto-Uchiyama encryption scheme and Paillier cryptosystem, and some of $\overline{X}_i^{\overline{W}}$ should be packed in one message $\overline{M}$;

$$\overline{M} = \overline{X}_i^{\overline{W}} || \overline{X}_{i+1}^{\overline{W}} || \cdots || \overline{X}_{i+\xi-1}^{\overline{W}}, \tag{42}$$

where ξ is the number of packed coefficients and is dependent on s_w and s_x. Such a packing operation is easily performed by computing the $\ell_x t$-th power of $E_{pk}(\overline{X}_{i+t}^{\overline{W}})$;

$$E_{pk}(\overline{M}) = \prod_{t=0}^{\xi-1} \left(E_{pk}(\overline{X}_{i+t}^{\overline{W}}) \right)^{\ell_x t} \tag{43}$$

The appropriate size of s_w and s_x are explored by implementing on a computer and evaluating the simulated performance. It is worth mentioning that the enciphering rate of Paillier cryptosystem approaches asymptotically 1 using the extension of the cryptosystem Damgård & Jurik (2001) and then more data can be packed in one ciphertext. Although the works in Fouque et al. (2003); Orlandi et al. (2007) can encode rational numbers by a limited precision, they are not suitable for the packing operation.

6. Simulation Results

Since the basic algorithm of our scheme is Cox's scheme with a limited precision, we evaluate the degradation of image quality by PSNR, and the detected correlation values compared with the original values. If the results are similar, we regard that the performance is not degraded. In our simulation, a standard gray-scaled image "lena" of 256 × 256 pixels is used. The length of watermark signal W is $\ell = 1000$ and the embedding intensity is $\alpha = 0.1$. Even if p_w and

p_x are added, the values of w_i and x_i might be negative. In such a case, the values are simply rounded to 0.

The comparison of PSNR and correlation values for the watermarked image which is not distorted by attacks are shown in Fig.6 and Fig.7, respectively. The PSNR of original Cox's scheme is 34.93 [dB] and the correlation value is 31.91, which are drawn by dot line in the figures. From the figures, we can see that the performance is asymptotically reaching the original value according to the increase of the scaling factors s_w and s_x. As the basic algorithm is Cox's scheme with a limited precision, we can regard that the performance is not degraded when the detected correlation values are similar.

One of the important characteristic in the spread spectrum watermarking technique is the orthogonality of each watermark signal because of the robustness against collusion attack. It is well-known that the original scheme retains the robustness with a dozen of colluders. Under averaging collusion with 5 users, the average similarity value of original scheme is 13.64, and the proposed one is shown in Fig.8. The robustness against the combination of collusion attack and JPEG compression are compared, which results are shown in Fig.9. From the results, the degradation of performance from the original scheme is very slight, and it does not affect the robustness against attacks. It is noted that the scaling factors s_w and s_x are closely related to the degradation of performance. It is better to increase the value of these parameters, for example $s_w \geq 2^3$ and $s_x \geq 2^3$, but we have to consider the communication costs because the bit-length to represent the watermarked DCT coefficient $\overline{X}_i + \overline{\alpha}_i \overline{w}_i$ is increased according to the size of s_w and s_x, which degrades the coding rate of such information. For other images, "aerial", "baboon", "barbala", "f16", "girl", and "peppers", the similar results are derived with the above parameters as shown in Table 2 and 3. The attenuation of PSNR value from the original one is at most 0.1%, that of the correlation value is at most 0.3%, and under averaging collusion the attenuation is less than 1%. As the consequence, recommended parameters are $s_w = 2^3$ and $s_x = 2^3$ from the simulation results.

When we use the above recommended parameters, the value of $\overline{X}_i^{\overline{W}}$ can be represented by 20 bits (the range must be within [0, 2^{20}] if $s_w = s_x = 2^3$). For the security reason, the bit-length of a composite $n = pq$ for the modulus of Paillier cryptosystem should be no less than 1024 bits. When $|n| = 1024$, an 1024-bit message is encrypted to an 2048-bit ciphertext. Under the above condition, the number of watermarked DCT coefficients in one ciphertext is at most 51 $(= \lfloor 1024/20 \rfloor)$. Since the number of DCT coefficients are $65536 = 256 \times 256$, the number of ciphertexts is 1286 $(= \lfloor 65536/51 \rfloor)$ and the total size of the ciphertexts is about 2.5MB, which is about 40 times larger than the original file size 66KB. In case the packing is not performed, the total size is more than 128MB. Therefore, we can conclude that the proposed method efficiently implements the Cox's spread spectrum watermarking scheme in the asymmetric fingerprinting protocol.

7. Conclusion

In this chapter, we investigated an asymmetric fingerprinting protocol with additive homomorphism and a method for implementing watermarking technique in an encrypted domain for assuring the asymmetric property of fingerprinting system. We developed the commitment scheme utilized to achieve the asymmetric property, and enhance the enciphering rate by applying Okamoto-Uchiyama encryption scheme for the cryptographic protocol that retains additive homomorphism. In order to contain information in one ciphertext as much as possible, the large message space is effectively partitioned by multiplexing each fingerprinted and encrypted component of an image.

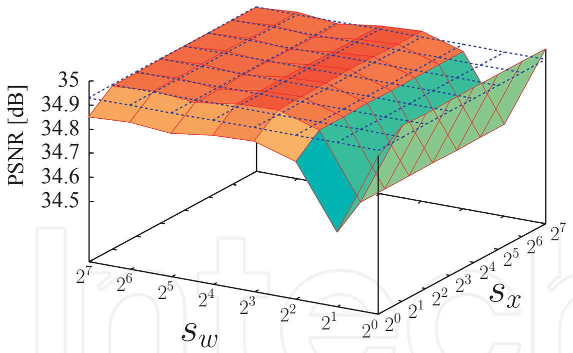

Fig. 6. The image quality for the scaling values s_w and s_x, where that of original scheme is 34.93 [dB] depicted by dot lines.

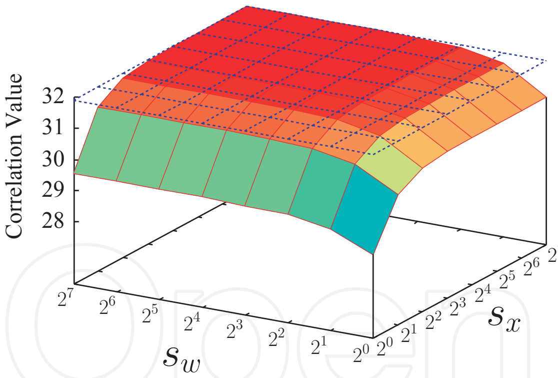

Fig. 7. The correlation values for the scaling values s_w and s_x, where that of original scheme is 31.90 depicted by dot lines.

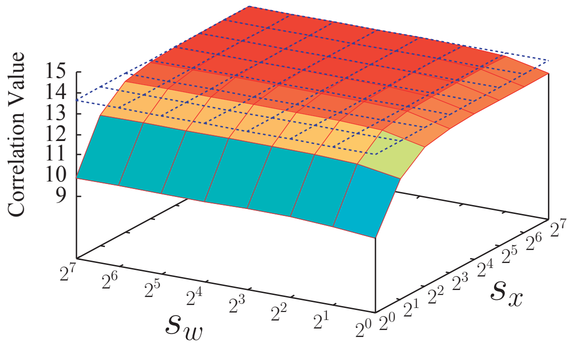

Fig. 8. The average correlation value after averaging collusion attack for the scaling values s_w and s_x.

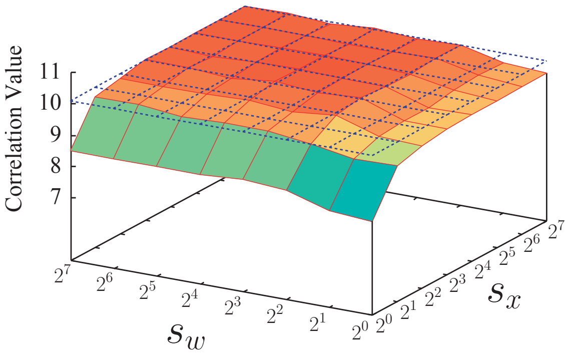

Fig. 9. The average correlation value after averaging collusion attack and JPEG compression with quality 35% for the scaling values s_w and s_x, where the average value of original scheme is 10.10.

We proposed a new of approaches for collaborating the proposed asymmetric fingerprinting protocol and watermarking technique. In the conventional implementation, the QIM watermarking is applied to the fingerprinting protocol exploiting the quantization procedure that truncates a real value to integer, which is unavoidable process to apply the public-key cryptosystem based on the algebraic property of integer. In the method, fingerprint information must be coded by a fingerprinting code to be robust against collusion attack. It also causes another issues such that the applicable contents are limited to huge contents like movie because of the long code-length. In this chapter, we implemented the spread spectrum watermarking to be applicable for various kinds of contents. After exploring the fundamental properties of signals in an encrypted domain, a fingerprint sequence is scaled up in order not to attenuate the signal energy by quantization. Moreover, the effects of rounding operation that maps a real value into a positive integer are formulated, and an auxiliary operation to obtain a watermarked image is presented. From our simulation results, the identification capability of our algorithm is quite similar to the original spread spectrum watermarking scheme, hence we can simulate the scheme on the cryptographic protocol with a limited precision.

	aerial	baboon	barbala	f16	girl	lena	peppers
original	36.34	34.96	34.61	35.59	35.49	34.96	34.48
proposed	36.35	34.95	34.61	35.59	35.48	34.95	34.48

Table 2. The degradation of the image quality when $s_w = s_x = 2^3$.

		aerial	baboon	barbala	f16	girl	lena	peppers
No attack	original	31.91	31.91	31.91	31.91	31.87	31.91	31.91
	proposed	31.87	31.82	31.85	31.85	31.79	31.84	31.85
Collusion	original	13.66	13.64	13.65	13.65	13.54	13.64	13.65
	proposed	13.61	13.50	13.54	13.57	13.40	13.54	13.55
Collusion + JPEG 35%	original	11.60	9.14	8.95	9.74	9.01	10.10	10.27
	proposed	11.56	9.18	8.91	9.73	9.18	10.06	10.16

Table 3. The degradation of the correlation values when $s_w = s_x = 2^3$.

8. References

Boneh, D. & Shaw, J. (1998). Collusion-secure fingerprinting for digital data, *IEEE Trans. Inf. Theory* **44**(5): 1897–1905.

Brassard, G., Chaum, D. & Crepeau, C. (1988). Minimum disclosure proofs of knowledge, *Journal of Computer and System Sciences* **37**: 156–189.

Chen, B. & Wornel, G. W. (2001). Quantization index modulation: a class of provably good methods for digital watermarking and information embedding, *IEEE Trans. Inform. Theory* **47**(4): 1423–1443.

Cox, I. J., Kilian, J., Leighton, F. T. & Shamson, T. (1997). Secure spread spectrum watermarking for multimedia, *IEEE Trans. Image Process.* **6**(12): 1673–1687.

Damgård, I. & Jurik, M. (2001). A generalisation, a simplification and some applications of paillier's probabilistic public-key system, *Proc. of PKC '01*, Vol. 1992 of *LNCS*, Springer-Verlag, pp. 119–136.

Fouque, P. A., Stern, J. & Wackers, G. J. (2003). Cryptocomputing with rationals, *Proc. of Finalcial Cryptography*, Vol. 2357 of *LNCS*, Springer-Verlag, pp. 136–146.

Goldwasser, S. & Micali, S. (1984). Probabilistic encryption, *JCSS* **28**(2): 270–299.

Katzenbeisser, S. & Petitcolas, F. A. P. (2000). *Information hiding techniques for steganography and digital watermarking*, Artech house publishers.

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

Lei, C., Yu, P., Tsai, P. & Chan, M. (2004). An efficient and anonymous buyer-seller watermarking protocol, *IEEE Trans. Image Process.* **13**(12): 1618–1626.

Memon, N. & Wong, P. W. (2001). A buyer-seller watermarking protocol, *IEEE Trans. Image Process.* **10**(4): 643–649.

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

Orlandi, C., Piva, A. & Barni, M. (2007). Oblivious neural network computing via homomorphic encryption, *EURASIP J. Inform. Security* **2007**(9).

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

Pfitzmann, B. & Sadeghi, A. (1999). Coin-based anonymous fingerprinting, *Advances in Cryptology – EUROCRYPT'99*, Vol. 1592 of *LNCS*, Springer-Verlag, pp. 150–164.

Pfitzmann, B. & Sadeghi, A. (2000). Anonymous fingerprinting with direct non-repudiation, *Advances in Cryptology – ASIACRYPT'2000*, Vol. 1976 of *LNCS*, Springer-Verlag, pp. 401–414.

Pfitzmann, B. & Schunter, M. (1996). Asymmetric fingerprinting, *Advances in Cryptology – EUROCRYPT'96*, Vol. 1070 of *LNCS*, Springer-Verlag, pp. 84–95.

Pfitzmann, B. & Waidner, M. (1997). Anonymous fingerprinting, *Advances in Cryptology – EUROCRYPT'97*, Vol. 1233 of *LNCS*, Springer-Verlag, pp. 88–102.

Prins, J. P., Erkin, Z. & Lagendijk, R. L. (2007). Anonymous fingerprinting with robust QIM watermarking techniques, *EURASIP J. Inform Security* **2007**(8).

Rivest, R. L., Shamir, A. & Adleman, L. (1978). A method for obtaining digital signatures and public key cryptosystems, *Commun. ACM* **21**(2): 120–126.

Staddon, J. N., Stinson, D. R. & Wei, R. (2001). Combinatiorial properties of frameproof and traceability codes, *IEEE Trans. Inform. Theory* **47**(3): 1042–1049.

Swaminathan, A., He, S. & Wu, M. (2006). Exploring QIM based anti-collusion fingerprinting for multimedia, *Proc. of SPIE, SPIE Conference on Security, Watermarking and Steganography*, p. 60721T.

Tardos, G. (2003). Optimal probabilistic fingerprint codes, *Proc. 35th ACM Symp. Theory of Comp.*, pp. 116–125.

Trappe, W., Wu, M., Wang, Z. J. & Liu, K. J. R. (2003). Anti-collusion fingerprinting for multimedia, *IEEE Trans. Signal Process.* **51**(4): 1069–1087.

Wang, Z. J., Wu, M., Trappe, W. & Liu, K. J. R. (2004). Group-oriented fingerprinting for multimedia forensics, *EURASIP J. Appl. Signal Process.* **2004**(14): 2142–2162.

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

Wu, M., Trappe, W., Wang, Z. J. & Liu, K. J. R. (2004). Collusion resistant fingerprinting for multimedia, *IEEE Signal Processing Mag.* pp. 15–27.

Yacobi, Y. (2001). Improved boneh-shaw content fingerprinting, *Proc. CT-RSA*, Vol. 2020 of *LNCS*, Springer-Verlag, pp. 378–391.

Zhao, H. V., Wu, M., Wang, Z. J. & Liu, K. J. R. (2005). Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting, *IEEE Trans. Image Process.* **14**(5): 646–661.

Zhu, Y., Feng, D. & Zou, W. (2005). Collusion secure convolutional spread spectrum fingerprinting, *Proc. IWDW2005*, Vol. 3710 of *LNCS*, Springer-Verlag, pp. 67–83.

Signal Processing
Edited by Sebastian Miron

ISBN 978-953-7619-91-6
Hard cover, 528 pages
Publisher InTech
Published online 01, March, 2010
Published in print edition March, 2010

This book intends to provide highlights of the current research in signal processing area and to offer a snapshot of the recent advances in this field. This work is mainly destined to researchers in the signal processing related areas but it is also accessible to anyone with a scientific background desiring to have an up-to-date overview of this domain. The twenty-five chapters present methodological advances and recent applications of signal processing algorithms in various domains as telecommunications, array processing, biology, cryptography, image and speech processing. The methodologies illustrated in this book, such as sparse signal recovery, are hot topics in the signal processing community at this moment. The editor would like to thank all the authors for their excellent contributions in different areas of signal processing and hopes that this book will be of valuable help to the readers.

How to reference
In order to correctly reference this scholarly work, feel free to copy and paste the following:

Minoru Kuribayashi (2010). Recent Fingerprinting Techniques with Cryptographic Protocol, Signal Processing, Sebastian Miron (Ed.), ISBN: 978-953-7619-91-6, InTech, Available from: http://www.intechopen.com/books/signal-processing/recent-fingerprinting-techniques-with-cryptographic-protocol

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821