Fingerprinting protocol for images based on additive homomorphic property

Kuribayashi, Minoru

Tanaka, Hatsukazu

Fingerprinting Protocol for Images Based on Additive Homomorphic Property

Minoru Kuribayashi, *Member, IEEE,* and Hatsukazu Tanaka, *Fellow, IEEE*

***Abstract*—Homomorphic property of public-key cryptosystems is applied for several cryptographic protocols, such as electronic cash, voting system, bidding protocols, etc. Several fingerprinting protocols also exploit the property to achieve an asymmetric system. However, their enciphering rate is extremely low and the implementation of watermarking technique is difficult. In this paper, we propose a new fingerprinting protocol applying additive homomorphic property of Okamoto–Uchiyama encryption scheme. Exploiting the property ingenuously, the enciphering rate of our fingerprinting scheme can be close to the corresponding cryptosystem. We study the problem of implementation of watermarking technique and propose a successful method to embed an encrypted information without knowing the plain value. The security can also be protected for both a buyer and a merchant in our scheme.**

***Index Terms*—Additive homomorphic property, enciphering rate, fingerprinting protocol, quantization method, watermark.**

I. Introduction

ACCORDING to the development of the Internet and multimedia contents, such as music, pictures, movies, etc., are treated by digital formats on the network. It enables us to easily purchase digital contents via the net. However, it causes several problems, such as violation of ownership and illegal distribution of the copy. Watermarking [1] is one of the effective schemes to solve these problems. It enables the owner to embed some information in the contents and to extract it. The semantic of the embedded information helps classifying the different applications. When the information indicates a copyright owner, it is applied for the ownership protection. A fingerprinting scheme embeds the information related to a buyer and enables a merchant to trace the buyer from the redistributed copy. First, a symmetric fingerprinting scheme has been proposed [2]. In the scheme, a merchant embeds the buyer's identity in his contents by himself. In the scheme, the merchant may frame a legal buyer because the merchant can distribute the fingerprinted contents by himself as he possesses it and then may insist that the distributed contents is the same one sold to the buyer. Therefore, the merchant cannot prove the buyer's treachery to anyone. To solve the problem, some cryptographic methods were applied so that only a buyer can obtain the fingerprinted contents, which is called asymmetric fingerprinting [3], [4]. Furthermore, an anonymous fingerprinting scheme [5] was introduced to solve the condition that electronic market places should offer to the customers the same privacy as the real-world market places. The concept of anonymous fingerprinting introduced in [5] has been presented only general theorems, not any practical implementation. The explicit construction was shown in [6] and [7], which are based on digital coins. Since all operations are simple computations such as modular multiplications and exponentiations, it seems easy to implement for a real application. However, from the point of enciphering information rate, the efficiency is very bad. Therefore, the improvement of the enciphering rate is essential for the realization of the fingerprinting system. However, the enciphering rate has been neglected, and other factors required for the implementation has been discussed actively. Kim *et al.* [8] improved the computational costs using the bilinear Diffie–Hellman problem. In [9] and [10], they focused on the conspiracy attack, which is the collusion attack of trusted third party and a merchant.

On the asymmetric fingerprinting, homomorphic property of public-key cryptosystems is exploited to achieve the asymmetric property. If an operation "$*$" on the ciphertext space results in an operation "$\star$" on the message space, such crytosystem is called homomorphic. In the conventional schemes [5]–[7], a bit-commitment scheme [11], whose enciphering rate should be more than $1/10^3$ for security reasons, is applied to achieve the asymmetric property. If the data size of the contents is 1 MB, the amount of communication data is more than 1 GB, which is extremely inefficient. Therefore, it is inevitable to increase the enciphering rate, and, hence, a cryptosystem with a large message space should be applied to make an efficient fingerprinting protocol.

In order to embed fingerprinting information in the contents, a watermarking technique should be applied. However, in previous schemes [4], [8]–[10], how to embed encrypted information in encrypted contents and how to make the system robust against attacks is not deeply considered. We study both fingerprinting and watermarking techniques and find the following difficulty in the implementation. In watermarking techniques for digital images, it is desirable to embed information in the frequency components for both robustness and perceptual quality. However, as the frequency components are real numbers, there is a difficulty in applying cryptographic techniques directly because they are based on the algebraic property of an integer. In many watermarking schemes, an information bit is embedded in the frequency component by quantizing it to the nearest odd

Manuscript received November 4, 2003; revised November 21, 2004. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Benoit Macq.

M. Kuribayashi is with the Faculty of Engineering, Kobe University, Kobe 657-8501, Japan (e-mail: minoru@eedept.kobe-u.ac.jp; kminoru@kobe-u.ac.jp).

H. Tanaka is with the Kobe Institute of Computing, Kobe 650-0001, Japan (e-mail: tanaka@kic.ac.jp).

Digital Object Identifier 10.1109/TIP.2005.859383

or even number, depending on the information bit. However, it seems difficult to exploit the method without the knowledge of the information bit.

In this paper, we propose a new construction scheme of anonymous fingerprinting that improves the enciphering rate by exploiting Okamoto–Uchiyama encryption scheme [12]. The fingerprinting protocol is analyzed in the outline of [13], and one explicit implementation method is introduced, which is an improved watermarking method of [14]. Since the Okamoto–Uchiyama encryption scheme has an additive homomorphic property, the multiplication of an encrypted fingerprint and an encrypted digital image is equivalent to embed a fingerprint in the digital image. The property enables a merchant to embed a buyer's identity information in the ciphertext of his image. In the protocol, the buyer can convince the merchant that his ciphertext really includes his identity without informing the plain value, and, hence, the anonymity of the buyer is established. The trade between a buyer and a merchant is executed as follows. A buyer encrypts his fingerprint and commits it to a merchant using zero-knowledge proofs. The merchant embeds the received data in his encrypted digital image and returns it to the buyer. Finally, the buyer decrypts and gets the fingerprinted contents without disclosing the fingerprint to the merchant. As a result, only the buyer gets the fingerprinted image unless he redistributes it. Considering the robustness against attacks, the fingerprint should be embedded in the frequency components. As such components are real values, all frequency components of an image are quantized to integers so as to apply the cryptosystem. For watermarking techniques, a quantization method is useful in our system as a fingerprint can be embedded when the coefficients are quantized. In order to preserve the perceptual quality of the fingerprinted image, each component is quantized adaptively by a specially customized quantization step size. As a quantization table used in the JPEG compression algorithm is designed considering human perceptual property, we modify the table so that it is applicable for our embedding scheme, and in order to embed an information bit which value is unknown, the frequency components in the embedding positions are quantized to the nearest even number before embedding so that the value can be changed, depending on the information bit. Furthermore, our system can achieve the same enciphering rate as that of applied cryptosystem by suitably designing the message space of a ciphertext.

The rest of this paper is organized as follows. In Section II, we review fingerprinting protocols and discuss the drawbacks of the conventional schemes briefly. Our proposed fingerprinting protocol and embedding protocol are described in Sections III and IV, respectively. Several computer simulation results are shown in Section V, and the improvement of the enciphering rate is discussed in Section VI. Finally, we conclude this paper.

II. Fingerprinting

In this section, we introduce some basic techniques used in our scheme. First, we review and classify the fingerprinting techniques. Then, bit-commitment schemes that are exploited in the conventional schemes are reviewed, and some inherent problems are disclosed. Finally, the Okamoto–Uchiyama encryption scheme is summarized in order to refer the encryption and decryption functions and their properties.

A. Classification

Digital contents, such as pictures, music, movies, etc., are easily copied without any degradation. Fingerprinting is a cryptographic scheme for the copyright protection of digital contents assisted by a watermarking technique, and the scheme can dissuade people from executing illegal redistribution of digital contents by making it possible for the merchant to identify the original buyer of the redistributed copy, where we call him a "traitor." The fingerprinting schemes are classified into the following three classes.

Symmetric: The operation to embed a fingerprint is performed only by a merchant. 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 merchant. After the sale, only the buyer obtains contents with a fingerprint. If the merchant finds the fingerprinted copy somewhere, he can identify the traitor and prove it to the third party.

Anonymous: A buyer can purchase fingerprinted contents without informing his identity to a merchant, but the merchant 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 merchant; otherwise, he can produce fingerprinted contents by himself. Therefore, an interactive protocol is performed to prevent the merchant from obtaining fingerprinted contents. The protocol is based on public-key cryptosystems, because they assurethat only a buyer can decrypt a ciphertext, though both of them can perform the enciphering operation. In order to achieve the asymmetric fingerprinting, the homomorphic property of public-key cryptosystems is applied.

B. Homomorphic Property

The homomorphic property of public-key cryptosystems is often applied for cryptographic protocols, as operations 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 following three operations, "*addition, multiplication, or exclusive*," in public-key cryptosystems. Therefore, the discussion in this section is focused on only such operations.

Let $E(m)$ be a ciphertext of a message m. Then, the homomorphic property satisfies the following equation:

$$E(m_1) \cdot E(m_2) = E(f(m_1, m_2)) \tag{1}$$

where $f(\cdot)$ is one of the above three operations. If m_1 is regarded as digital contents and m_2 as a watermark, the encrypted information can be embedded in the encrypted contents. Generally, when a watermark is embedded in an image, the marking positions, like frequency components, are determined by a secret key for the security against the intentional manipulation. So, m_2

must be the value of such positions instead of the whole image. For example, all frequency components are encrypted, and then several components specified by a secret key are watermarked by multiplying the encrypted watermark. As a result, the manipulation/removal of the watermark becomes difficult.

In the asymmetric fingerprinting scheme, a buyer and a merchant jointly embed a fingerprint. First, the buyer encrypts a fingerprint and sends it to the merchant. Then, the merchant verifies that the received ciphertext is made from the real fingerprint, and embeds it in his encrypted contents by multiplying those ciphertexts. Finally, the buyer receives the encrypted and fingerprinted contents and decrypts them. After the protocol, only the buyer gets the fingerprinted contents without disclosing his identity. Memon and Wong [4] apply the multiplicative property of RSA scheme [15] to embed the fingerprint and Pfitzmann *et al.* [6], [7] and exploit bit -commitment schemes based on the quadratic residues [11]. In the latter scheme, a buyer can convince a merchant that a transmitted ciphertext really contains his fingerprinting information using zero-knowledge proof. Such a characteristic is necessary for security reasons, and the anonymity of a buyer is achieved.

C. Overview of Pfitzmann's Scheme

Pfitzmann *et al.* [5] have constructed an anonymous fingerprinting system by several protocols. There are three parties: buyer $\mathcal{B}$, merchant $\mathcal{M}$, and registration center $\mathcal{RC}$. First, $\mathcal{RC}$ generates two kinds of keys, secret keys and public keys, and distributes the latter to all participants of the system. When $\mathcal{B}$ begins a trade to a merchant $\mathcal{M}$, first $\mathcal{B}$ must register at $\mathcal{RC}$. And then $\mathcal{B}$ withdraws a digital coin which includes a identify proof $W = g^{id}$ 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 it to $\mathcal{M}$. Then, using a zero-knowledge proof, $\mathcal{B}$ proves that the contents of the ciphertext is equivalent to that of W. After $\mathcal{M}$ 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, using the zero-knowledge proof, that the ciphertext really includes fingerprint, two kinds of bit-commitment schemes are applied. One is based on the discrete logarithm assumption and the other is on the quadratic residues [11], for which security depends on the p-subgroup assumption and the quadratic residues assumption, respectively. We call the commitment schemes BC_{DL} and BC_{RQ}, respectively, and review them briefly.

BC_{DL}: Let p be a large prime and g and h be the generators. The commitment $\mathrm{com1}$ of a bit b is calculated using a random number r as follows:

$$\mathrm{com1} = g^b h^r (\mathrm{mod} p). \tag{2}$$

BC_{QR}: Let p and q be large primes and $n = pq$. The commitment $\mathrm{com2}$ is obtained by the following equation:

$$\mathrm{com2} = (-1)^b r^2 (\mathrm{mod} n). \tag{3}$$

Here, it is remarkable that the committed value b of BC_{DL} is not only binary, it can take an integer of $(\boldsymbol{Z}/p\boldsymbol{Z})$. When W is calculated based on BC_{DL}, then it is difficult for a merchant to embed directly the value of id which is the contents of W. Because the recovery of the committed value is impossible for the commitment scheme, and when a watermark information is embedded, each bit of the information is operated to an image. So, instead of W, the commitment of each information bit of id, which is calculated by BC_{QR}, is applied for embedding. Then, a buyer must certify that the values of the commitments are equivalent to that of W. Using BC_{DL}, $\mathcal{B}$ convinces $\mathcal{M}$ by zero-knowledge interactive protocol that the committed value of $\mathrm{com1}$ is equivalent to that of $\mathrm{com2}$. Therefore, two commitment schemes are required in the conventional scheme.

After the above protocol, only $\mathcal{B}$ can decrypt the fingerprinted contents and $\mathcal{M}$ 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 contents, 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. To improve the rate, we propose a new method based on the Okamoto–Uchiyama encryption scheme [12].

D. Okamoto–Uchiyama Encryption Scheme

Let p and q be two large primes ($|p| = |q| = k$ bits) and $N = p^2 q$. Choose $g \in_R (\boldsymbol{Z}/N\boldsymbol{Z})$ 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 is (N, g, h, k), and a secret key is (p, q).

The cryptosystem, based on the exponentiation $\mathrm{mod}N$, is constructed as follows.

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

$$C = g^m h^r (\mathrm{mod} N). \tag{4}$$

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

$$m = \frac{L(C_p)}{L(g_p)} (\mathrm{mod} p) \tag{5}$$

where

$$L(x) = \frac{x-1}{p}. \tag{6}$$

We denote the encryption function $E(m, r)$ and decryption function $D(C)$. Three important properties of the scheme are given by the following: P1, P2, and P3.

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

$$E(m_1, r_1) \cdot E(m_2, r_2) = E(m_1 + m_2,\ r_1 + r_2) (\bmod N). \tag{7}$$

P2. It is semantically secure if the following assumption, *i.e.*, p-subgroup assumption, is true: $E(0, r) = h^r \bmod$

N and $E(1, r') = gh^{r'} \bmod N$ is computationally indistinguishable, where r and r' are uniformly and independently selected from $\in_R (\boldsymbol{Z}/N\boldsymbol{Z})$.

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

In our fingerprinting protocol, the additive homomorphic property of Okamoto–Uchiyama encryption scheme is ingeniously applied. Concerning to the enciphering rate, our scheme can be close to the rate of Okamoto–Uchiyama encryption scheme, which is 1/3. Paillier cryptosystem [16] has the similar structure to Okamoto–Uchiyama encryption scheme. Although the enciphering rate is higher, it requires more computations. So, the selection of the scheme is dependent on the applied system. For convenience, all protocol in our scheme is based on the Okamoto–Uchiyama encryption scheme, and the notation used here is used in the following section. Since our approach can be easily translated to the Paillier cryptosystem, the detail is omitted in our paper.

III. Proposed Fingerprinting Protocol

The idea of our proposed scheme is to exploit the Okamoto–Uchiyama encryption scheme for anonymous fingerprinting. If we assume that a fingerprint is denoted by a number m_1 and a digital image is given by a number m_2, then a fingerprinted item becomes $m_1 + m_2$. In our scheme, a buyer $\mathcal{B}$ can commit his identity to a merchant $\mathcal{M}$ as a fingerprint without informing the real value, and $\mathcal{M}$ can embed the fingerprint in the image at the enciphered form. After receiving the encrypted and fingerprinted image, $\mathcal{B}$ decrypts it, but cannot remove the fingerprint. The protocol is shown briefly in Fig. 1.

A. Fingerprinting Protocol

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

[Fingerprinting Protocol]

Step 1. $\mathcal{M}$ 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 $a_j \in_R (\boldsymbol{Z}/N\boldsymbol{Z})$ to satisfy the following equation:

$$a = \sum_{j=0}^{\ell-1} a_j 2^j \tag{8}$$

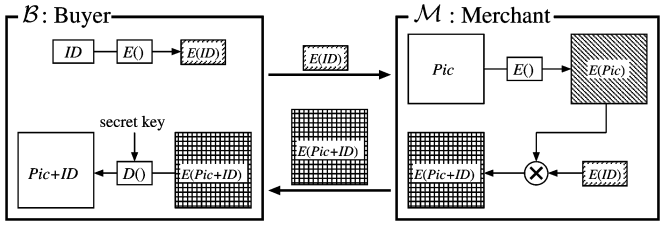

Fig. 1. Our protocol model.

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

$$\sum_{j=1}^{\ell-1} a_j 2^j < a \tag{9}$$

and a_0 is calculated as follows:

$$a_0 = a - \sum_{j=1}^{\ell-1} a_j 2^j. \tag{10}$$

A bit commitment of each w_j is calculated as

$$\mathrm{com}_j = g^{w_j} h^{a_j} (\mathrm{mod} N) \tag{11}$$

$$= E(w_j, a_j)(\mathrm{mod} N) \tag{12}$$

and sent to $\mathcal{M}$.

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

$$V = h^a (\mathrm{mod} N) \tag{13}$$

and makes sure that the following equation can be satisfied:

$$\prod_j \mathrm{com}_j{}^{2^j} \stackrel{?}{=} W \cdot V (\mathrm{mod} N). \tag{14}$$

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

$$Y_i = \begin{cases} g^{I_i} h^{b_i} \cdot \mathrm{com}_j^T (\mathrm{mod} N), & \text{marking position} \\ g^{I_i} h^{b_i} (\mathrm{mod} N), & \text{elsewhere} \end{cases} \tag{15}$$

and sends it to $\mathcal{B}$.

Step 5. Since the received Y_i is rewritten as

$$Y_i = \begin{cases} g^{(I_i + Tw_j)} h^{Ta_j + b_i} (\mathrm{mod} N), & \text{marking position} \\ g^{I_i} h^{b_i} (\mathrm{mod} N), & \text{elsewhere.} \end{cases} \tag{16}$$

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

$$D(Y_i) = \begin{cases} I_i + Tw_j (\mathrm{mod} p), & \text{marking position} \\ I_i (\mathrm{mod} p), & \text{elsewhere.} \end{cases} \tag{17}$$

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

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

$$\mathrm{com}_j^T = (g^{w_j} h^{a_j})^T (\mathrm{mod} N)$$

$$= g^{Tw_j} h^{Ta_j} (\mathrm{mod} N)$$

$$= E(Tw_j, Ta_j). \tag{18}$$

In watermarking schemes [1], a watermark is added to or subtracted from pixel values or frequency components with a cer-

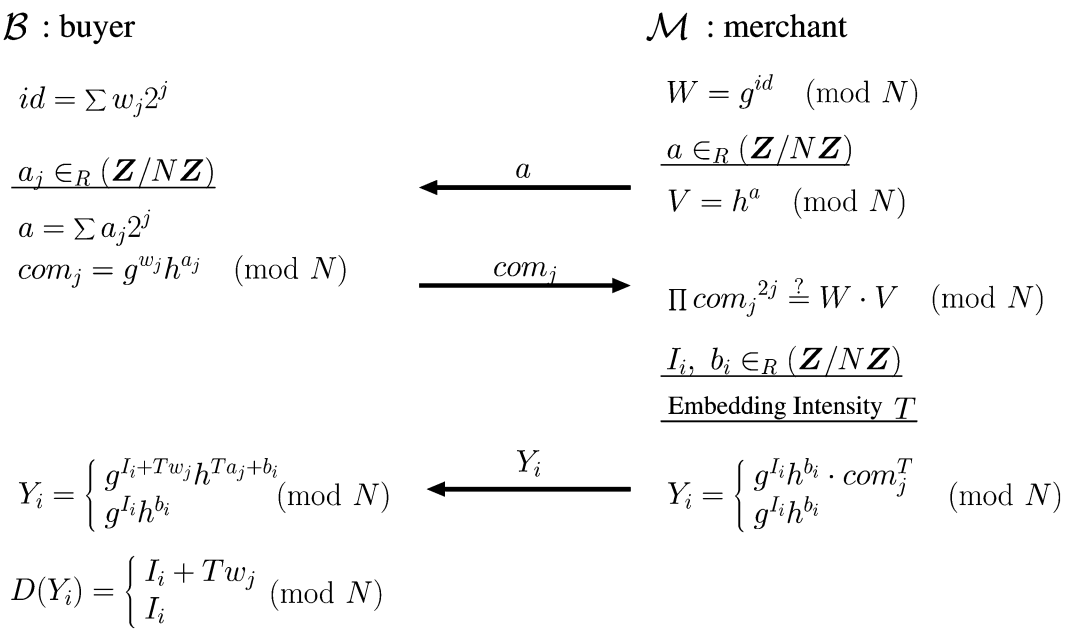

Fig. 2. Fingerprinting protocol.

tain intensity. Therefore, the characteristic of our scheme is suitable for such watermark schemes. In (15), $g^{I_i} h^{b_i} = E(I_i, b_i)$ is regarded as $\mathcal{M}$'s enciphered image, and then from the property P1 Y_i, the marking position is rewritten as

$$\begin{aligned} Y_i &= E(I_i, b_i) \cdot E(Tw_j, Ta_j) \\ &= E(I_i + Tw_j, Ta_j + b_i). \end{aligned} \tag{19}$$

If $\mathcal{M}$ uses I_i as a pixel value directly, the above operation can be applied easily. Considering the robustness against attack, such as lossy compression and filtering operations, etc., the transformed domain is generally more resilient against such attacks. However, if $\mathcal{M}$ applies the transformed coefficients, the message should be modified for the adaptive data structure; the detail is discussed in Section IV.

B. Binary Proof

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, (14) 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, we propose a zero-knowledge interactive protocol to prove that a commitment contains binary values. As a commitment scheme is basically a tool for zero-knowledge proof, our protocol applies the property. An excellent point of the protocol is that both the buyer and the merchant calculate a commitment by modifying the original commitment com_j. The protocol is described as follows (indicated in Fig. 3).

[Binary Proof]

Step 1. In order to check com_j, $\mathcal{M}$ generates random numbers t_j and c_j, such that $t_j + c_j$ is less than 2^{k-1}, calculates

$$\mathrm{COM}_j = \mathrm{com}_j^{t_j} \cdot g^{c_j} (\mathrm{mod} N) \tag{20}$$

and sends it to $\mathcal{B}$.

Step 2. $\mathcal{B}$ decrypts the received COM_j as

$$D(\mathrm{COM}_j) = w_j t_j + c_j (\mathrm{mod} N) \tag{21}$$

and then he generates a random number $r_j \in_R (\boldsymbol{Z}/N\boldsymbol{Z})$ and calculates

$$\widehat{\mathrm{com}}_j = \mathrm{com}_j^{t_j + c_j} \cdot h^{r_j} (\mathrm{mod} N) \tag{22}$$

using the values w_j, a_j, COM_j, and $D(\mathrm{COM}_j)$. The detail is shown in the following Remark 2.

Step 3. After $\mathcal{M}$ receives $\widehat{\mathrm{com}}_j$, he sends t_j and c_j to prove that COM_j has been really produced using them.

Step 4. If (20) is satisfied for the received t_j and c_j, $\mathcal{B}$ sends r_j to $\mathcal{M}$. If it is not satisfied, he can claim $\mathcal{M}$'s fraud.

Step 5. By verifying (22), $\mathcal{M}$ can certified that com_j contains only 1-bit information.

Remark 2: If $w_j = 0$ in Step 2, then $D(\mathrm{COM}_j) = c_j$ and $\mathrm{COM}_j = g^{c_j} h^{a_j t_j} \bmod N$. Using COM_j and $D(\mathrm{COM}_j)$, $\mathcal{B}$ can calculate

$$\begin{aligned} \widehat{\mathrm{com}}_j &= \mathrm{COM}_j \cdot g^{-D(\mathrm{COM}_j)} h^{a_j D(\mathrm{COM}_j) + r_j} (\mathrm{mod} N) \\ &= g^{c_j} h^{a_j t_j} \cdot g^{-c_j} h^{a_j c_j + r_j} (\mathrm{mod} N) \\ &= h^{a_j (t_j + c_j) + r_j} (\mathrm{mod} N) \\ &= E(0, a_j (t_j + c_j) + r_j) \\ &= \mathrm{com}_j^{t_j + c_j} \cdot h^{r_j}. \end{aligned} \tag{23}$$

If $w_j = 1$, then $D(\mathrm{COM}_j) = t_j + c_j$. Therefore, $\widehat{\mathrm{com}}_j$ is obtained by the following:

$$\begin{aligned} \widehat{\mathrm{com}}_j &= g^{D(\mathrm{COM}_j)} h^{a_j D(\mathrm{COM}_j) + r_j} (\mathrm{mod} N) \\ &= g^{t_j + c_j} h^{a_j (t_j + c_j) + r_j} (\mathrm{mod} N) \\ &= E(t_j + c_j, a_j (t_j + c_j) + r_j) \\ &= \mathrm{com}_j^{t_j + c_j} \cdot h^{r_j}. \end{aligned} \tag{24}$$

$\mathcal{B}$ cannot calculate $\widehat{\mathrm{com}}_j$ using the decrypted COM_j because the knowledge of each t_j and c_j or $t_j + c_j$ is inevitable. Therefore,

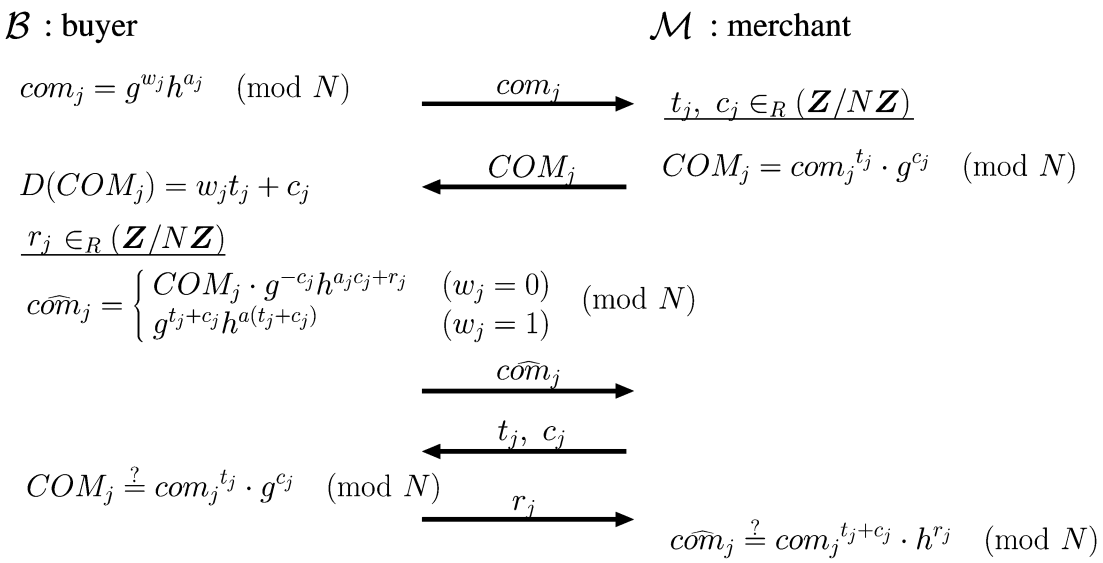

Fig. 3. Binary proof protocol.

the lack of information makes it impossible to calculate $\widehat{\mathrm{com}}_j$ when the values of w_j are not binary. From the above facts, the following lemma can be proved.

Lemma 1: $\mathcal{B}$ can prove that the values of w_j are binary using a zero-knowledge protocol if p-subgroup assumption is true.

Proof: $\mathcal{B}$ cannot obtain the values both t_j and c_j from COM_j, but only $w_j t_j + c_j$. For lack of information, the calculation of $t_j + c_j$ from w_j and $w_j t_j + c_j$ is extremely difficult if the values of w_j are not binary. Therefore, without the knowledge of t_j and c_j, it is difficult for $\mathcal{B}$ to calculate $\mathrm{com}_j^{t_j + c_j}$ except for only two cases described in Remark 2, and, hence, if (22) is satisfied, $\mathcal{M}$ cannot deny that the values of w_j are binary. And from the property P3, random number r_j changes the ciphertext $\mathrm{com}_j^{t_j + c_j}$ to $\mathrm{com}_j^{t_j + c_j} \cdot h^{r_j} = E\big(w_j(t_j + c_j),\ a_j(t_j + c_j) + r_j\big)$, preserving the plaintext $w_j(t_j + c_j)$. It guarantees that no information about w_j leaks to $\mathcal{M}$, as he cannot distinguish $E\big(0,\ a_j(t_j + c_j) + r_j\big)$ and $E\big(t_j + c_j,\ a_j(t_j + c_j) + r_j\big)$ from the property P2, which implies that the security of the commitment which is a ciphertext of Okamoto–Uchiyama encryption scheme is dependent on p-subgroup assumption. ■

C. Security

First, we consider the security concerning to $\mathcal{M}$. In the fingerprinting protocol, $\mathcal{B}$ can prove that the values of w_j are binary using the binary proof protocol from the Lemma 1, and, hence, $\mathcal{M}$ can embed $\mathcal{B}$'s identity properly and securely in his image if p-subgroup assumption is true. One possible attack is to remove or change the embedded identity information directly from a fingerprinted image, which is equivalent to attack the applied watermarking system. So, we can conclude that the security concerning to $\mathcal{M}$ is protected if the applied watermarking system is robust against attacks, and the p-subgroup assumption is true. Regretfully, the absolutely robust watermaring scheme dose not exist in nature. Watermarking only guarantees the robustness for a certain degree of image quality. If the quality is decreased too much, the extraction of a watermark may fail. Although the perfect robustness is impossible, it is really meaningful to achieve the higher.

In order to certify the security concerning $\mathcal{B}$, we must prove that $\mathcal{M}$ cannot obtain $\mathcal{B}$'s identity under the following three assumptions:

A1: The discrete logarithm problem is too difficult to solve.

A2: The Okamoto–Uchiyama encryption scheme is semantically secure.

A3 : $\mathcal{B}$ never redistributes a copy.

From these assumptions, the following theorem can be proved.

Theorem 1: $\mathcal{B}$ can purchase a digital image from $\mathcal{M}$ anonymously if three assumptions A1, A2, and A3 are satisfied.

Proof: As $W = g^{id} \bmod N$, to derive the identity id from W is equivalent to solve the discrete logarithm problem, but it is extremely difficult from the assumption A1. In Step 2 of the fingerprinting protocol, the bit commitment com_j has only two forms: one is $E(0,\ r)$ and the other is $E(1,\ r)$, as the values of w_j are binary. $\mathcal{M}$ cannot obtain the w_j from the commitment com_j if the assumption A2 is satisfied. Enabling $\mathcal{M}$ to get a fingerprint from illegally redistributed copy, the identity id is extracted from the decrypted Y_i. However, $\mathcal{M}$ never gets it under the assumption A3. Hence, the anonymity of $\mathcal{B}$ is preserved. ■

From Theorem 1, $\mathcal{M}$ cannot abuse the identity of $\mathcal{B}$. Therefore, the security concerning $\mathcal{B}$ is protected.

In each commitment com_j, the security depends on the p-subgroup assumption from (12) in our scheme; it is the same as Pfitzmann's scheme, and the encrypted and fingerprinted image in our scheme is Y_i, which is merely a ciphertext of the Okamoto–Uchiyama encryption scheme. So, the security depends on the difficulty of factoring N. On the other hand, the ciphertext of the conventional scheme is generated using a bit -commitment scheme, and the security depends on the quadratic residue assumption, which is stronger than the factoring assumption. Furthermore, the anonymity of a buyer can be proved in the *binary proof*, and the security depends on the

p-subgroup assumption, though there is no explicit protocol in the conventional schemes.

IV. How to Embed an Encrypted Information

A. Embedding

In order to embed an encrypted fingerprinting information bit in an encrypted image, the additive homomorphic property of public-key cryptosystems is applied. However, such public-key cryptosystems cannot use real values. Hence, watermarking schemes exploiting the frequency domain cannot be applied in the protocol directly. The analog values of frequency components should be quantized to an integer so as to use cryptographic applications.

In the quantization process, frequency components are quantized to the nearest integer. Then, in order to embed watermark information bits, several frequency components selected by a secret key, and quantized the special nearest even/odd number which is a multiple of a quantizing step. However, there is a serious problem in such embedding processes. In the asymmetric and anonymous fingerprinting, a merchant $\mathcal{M}$ cannot get a buyer $\mathcal{B}$'s plain identity information unless $\mathcal{B}$ shows it because each bit w_j of $\mathcal{B}$'s identity id is encrypted. In such a situation, it seems impossible for $\mathcal{M}$ to embed w_j in his image using the watermarking technique without knowing the plain value of w_j. On a quantization method, a coefficient is quantized to the nearest even number if $w_j = 0$, otherwise to the odd number. Without the knowledge of w_j, such a procedure cannot be performed. It is illustrated in Fig. 4.

Here, we propose one solution to embed an information bit w_j without knowing the plain value, which is easily applied for more complicated schemes. A frequency coefficient $f_{x,y}$ is first quantized to the nearest even numbers of a quantization step size $Q_{x,y}$

$$\overline{f_{x,y}} = \mathrm{int}_e\left(\frac{f_{x,y}}{Q_{x,y}}\right) \tag{25}$$

where $\mathrm{int}_e(\cdot)$ is a function that outputs the nearest even number. Here, the original value of the frequency coefficient should be considered for the following reason. If $f_{x,y}$ is less than the quantized coefficient $\overline{f_{x,y}}Q_{x,y}$, then $\overline{f}_{x,y} + w_j, (w_j = 1)$ is not the nearest odd number, and, hence, the degradation of the image is increased. So depending on the value of the coefficient, the following operation is calculated.

Case 1. If $f_{x,y}$ is more than $\overline{f_{x,y}}Q_{x,y}$, then

$$E(\overline{f_{x,y}}, b_i) \cdot E(w_j, a_j) = E(\overline{f_{x,y}} + w_j, b_i + a_j) (\mathrm{mod} N). \tag{26}$$

Case 2. else

$$E(\overline{f_{x,y}}, b_i) \cdot E(w_j, a_j)^{-1} = E(\overline{f_{x,y}} - w_j, b_i - a_j) (\mathrm{mod} N). \tag{27}$$

Calculating the above equation, the quantized frequency coefficient becomes an odd number if $w_j = 1$; otherwise, it is even number. So, even if the plain information bit is kept secret using cryptographic techniques, it is embedded in the frequency coefficient of an image. Therefore, depending on $f_{x,y}$, one of the above two equations is selected to embed an encrypted and fingerprinting information bit. In addition, if fingerprinting information is embedded in several special frequency coefficients selected by a secret key, it enhances the security against intentional alterations.

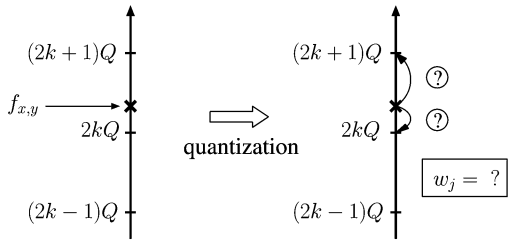

Fig. 4. Problem to embed an encrypted fingerprint.

In Step 4 of the fingerprinting protocol proposed in Section III, $\mathcal{M}$ performs the following operations to embed an encrypted fingerprint.

[Embedding]

Step 1. An image is partitioned into 16×16 blocks and each block is transformed by DCT.

Step 2. Using the $\mathcal{M}$'s secret key, several DCT coefficients are specified, and they are quantized to the nearest even number by quantizing step size $Q_{x,y}$

$$\overline{f_{x,y}} = \mathrm{int}_e\left(\frac{f_{x,y}}{Q_{x,y}}\right). \tag{28}$$

Other DCT coefficients are quantized to the nearest integer

$$\overline{f_{x,y}} = \mathrm{int}(f_{x,y}). \tag{29}$$

Step 3. Each quantized coefficient $\overline{f_{x,y}}$ is encrypted using the $\mathcal{B}$'s public key and a random number b_i. Then, the ciphertext is $E(\overline{f_{x,y}}, b_i)$.

Step 4. For the specified DCT coefficients, each fingerprinting information bit is embedded by multiplying two ciphertexts, as follows.

- If $f_{x,y} \geq \overline{f_{x,y}}Q_{x,y}$, then the ciphertext of the fingerprinted DCT coefficient $f'_{x,y}(= (\overline{f_{x,y}} \pm w_j)Q_{x,y})$ is calculated by the following operation:

$$\begin{aligned} E(f'_{x,y}, r') &= \left(E(\overline{f_{x,y}}, b_i) \cdot E(w_j, a_j)\right)^{Q_{x,y}} \\ &= \left(E(\overline{f_{x,y}} + w_j, b_i + a_j)\right)^{Q_{x,y}} \\ &= E\left((\overline{f_{x,y}} + w_j)Q_{x,y}, (b_i + a_j)Q_{x,y}\right). \end{aligned} \tag{30}$$

- Else, if $f_{x,y} < \overline{f_{x,y}}Q_{x,y}$, then

$$\begin{aligned} E(f'_{x,y}, r') &= \left(E(\overline{f_{x,y}}, b_i) \cdot E(w_j, a_j)^{-1}\right)^{Q_{x,y}} \\ &= \left(E(\overline{f_{x,y}} - w_j, b_i - a_j)\right)^{Q_{x,y}} \\ &= E\left((\overline{f_{x,y}} - w_j)Q_{x,y}, (b_i - a_j)Q_{x,y}\right). \end{aligned} \tag{31}$$

Step 5. The ciphertexts of the fingerprinted image are sent to $\mathcal{B}$.

When $\mathcal{B}$ received the ciphertexts, he first decrypts them, and then by performing IDCT, the fingerprinted image is obtained. In order to increase the robustness against attack, the embedding positions should not be selected from high-frequency coefficients because such coefficients are very sensitive for general

signal processing which may be performed by a hostile buyer, and if one information bit can be embedded being distributed in several coefficients, the robustness can be improved. Therefore, Step 3 of the merchant's operation is repeatedly performed α times for different low-frequency coefficients of several blocks so as to embed one information bit.

B. Quantization Table

When a fingerprint is embedded in an image, perceptual degradation should be considered. In our scheme, an image is first transformed to the frequency domain and then the components are quantized in order to apply cryptographic techniques which are based on the algebraic property of integer. Here, if the components quantized uniformly, the image quality must be degraded seriously. When a digital image is compressed by JPEG algorithm, a special quantization table shown in Table I is used. The table is designed to keep the perceptual quality as good as possible. So, the table is suitable for the quantization of an image. However, considering the robustness and the perceptual quality, the table size 8×8 is too small, because a watermark embedded in the block is vulnerable for the attack like the common signal processing. If a watermark is spread over a larger block, the robustness and the perceptual quality will be improved. Therefore, we reconstruct a larger quantization table based on the original one.

Let the original table be $q_{x,y}$, $(0 \leq x, y \leq 7)$. First, the table is expanded to horizontal direction, $b_{x,y}$, $(0 \leq x \leq 7, 0 \leq y \leq 15)$ as follows:

$$b_{x,y} = \begin{cases} q_{x,y/2} & (y = 0, 2, 4, \ldots, 14) \\ \frac{(q_{x,y/2} + q_{x,y/2+1})}{2} & (y = 1, 3, 5, \ldots, 13) \\ q_{x,7} & (y = 15). \end{cases} \tag{32}$$

and then it is expanded to vertical direction and $Q_{x,y}$, $(0 \leq x, y \leq 15)$ is obtained

$$Q_{x,y} = \begin{cases} b_{x/2,y} & (x = 0, 2, 4, \ldots, 14) \\ \frac{(b_{x/2,y} + b_{x/2+1,y})}{2} & (x = 1, 3, 5, \ldots, 13) \\ b_{15,y} & (x = 15). \end{cases} \tag{33}$$

where the fraction value is rounded by cutoff method.

When an image is compressed by JPEG algorithm, the quality is determined by selecting a quality parameter q_w. Using the parameter, the quantizing step size is calculated. Then, we must change the above procedure so as to be applicable for our quantization table as follows:

$$Q'_{x,y} = \frac{(100 - q_w)}{50} Q_{x,y}. \tag{34}$$

If the quality parameter q_w is decreased, the robustness against attack can can be improved, but the image quality will be decreased. So, it is necessary to consider the characteristic when the value of q_w is determined.

C. Extraction

Since the fingerprint is embedded by quantizing the DCT coefficients even/odd number, such information is extracted easily if one has the secret key which is used to specify the embedding position. When $\mathcal{M}$ finds an illegal copy, the information is extracted as follows. First, an image is transformed by DCT after partitioned into blocks, and then each coefficient in the embedding position is quantized using the corresponding quantization step size. If the value is even, the information bit is regarded as 0, otherwise 1. When one information bit is extracted from several DCT coefficients, the amount of even and odd numbers are counted. Then, the information bit is determined by the sum of those amount. Here, a more accurate extraction method may be possible as the following reason. Generally, the quantized DCT coefficients will be changed slightly after embedding because of the rounding error when IDCT is performed, and the common signal processing such as JPEG compression, filtering, etc., will affect the frequency coefficients. However, the above changes will not be so large, and, hence, the values of the DCT coefficients must contain the useful information to detect the the embedded information bit. Therefore, the analog information can be applied for such extraction procedure.

TABLE I
QUANTIZATION JPEG COMPRESSION

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

D. Consideration

Considering the robustness against common signal processing, one information bit is spread into α low-frequency components. It seems to sacrifice the security as a hostile buyer may be able to find the embedding positions. However, the above operation makes it more difficult for the following reasons. As the energy of the image is concentrated on the low DCT coefficients, such coefficients have large value and distribute randomly. Each DCT coefficient in the embedding positions is quantized by the special quantizing step size $Q'_{x,y}$ to the nearest even number and then information bit is embedded based on (26) or (27). So, the quantized value of each DCT coefficient is regarded as a random value, which makes difficult to identify the embedding positions from the fingerprinted coefficients. If one information bit is embedded in only one coefficient, it may be changed by the attack such that a buyer changes the randomly selected coefficients, but the possibility can be decreased if several coefficients are used to embed one information bit because a buyer must change more than $\alpha/2$ coefficients without loss of the perceptual quality. Further, as the number of DCT coefficients are much larger than that of information bit, there are a lot of candidates of the embedding positions for one information bit, and only the coefficients at the embedding positions are quantized even number, and such

quantized coefficients are changed by the fingerprint, which makes the coefficients randomly distributed.

For the evaluation of watermarking system, robustness against geometrical manipulation should be considered. One of the solutions for such attacks is to embed a synchronization signal so as to recover the loss of synchronization. In our scheme, it is possible to implement such resynchronization module before the fingerprinting protocol because the operation can be performed independently. A synchronization signal is embedded by $\mathcal{M}$ before the embedding of a fingerprint. When $\mathcal{M}$ finds an illegal copy, first the synchronization is recovered and then the extraction of a fingerprint is performed.

Several buyers may collude to analyze the embedding position by taking the difference of each fingerprinted image. One of the solutions is to embed noise in addition to a fingerprint so as to make the analysis difficult. Considering the payload for a still image, however, the acceptable number of coalitions will be small. Collusion secure codes [17] and anti-collusion codes [18] are designed to immunize against the analysis performed by colluded buyers. However, the length of those codes is extremely long; hence, it is impossible to embed such codes in a still image. If our scheme is applied for movie files, such codes may be able to use.

V. Simulation Results

In this section, we show several computer-simulated results. Concerning to the fingerprinting protocol, the validity can be proved by the security of Okamoto–Uchiyama encryption scheme, and it has already been proven in Section III. Therefore, the perceptual quality of the embedded image and the robustness against several attacks are shown in this section. In our simulation, we use a standard image "Lena" that has 256 level gray scale with size of 256×256, and the watermark information is 32 bits. Considering the robustness against signal processing attack, the size of α should be large. However, if α is increased too much, the candidates for the embedding positions are decreased. Hence, considering the tradeoff, we set $\alpha = 75$ in the following simulations.

If the quality factor q_w is decreased, the perceptual quality is also decreased accordingly. Fig. 5 shows the relation between q_w and PSNR. The robustness against attack is increased if q_w is decreased, but the perceptual quality is decreased. Therefore, there is a tradeoff between the robustness and perceptual quality and it should be considered to apply our scheme. Fig. 6 is the original image, and Fig. 7 is the fingerprinted image when $q_w = 55$ and $\alpha = 75$.

The robustness against JPEG compression is examined and the results are shown in Fig. 8, where the correct extraction rate means the the message extraction rate without error. From the results, the tolerance for JPEG compression is dependent on the value of q_w. Such value should be selected for the applied system. Concerning to the robustness against Gaussian filtering, the embedded information is extracted without any errors.

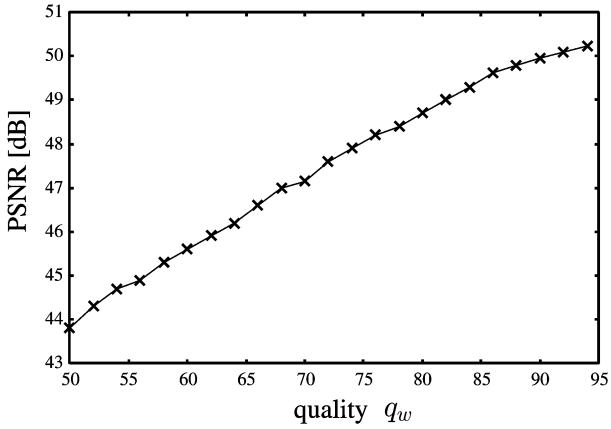

Fig. 5. PSNR versus quality q_w ($\alpha = 75$).

Fig. 6. Original image.

Fig. 7. Fingerprinted image ($\mathrm{PSNR} = 44.5$ dB).

VI. Improvement of the Enciphering Rate

A. Modified Fingerprinting Protocol

In the Section III, each I_i is encrypted and fingerprinted independently. Here, we consider the size of the message being encrypted, where the bit length of a message is revealed as the

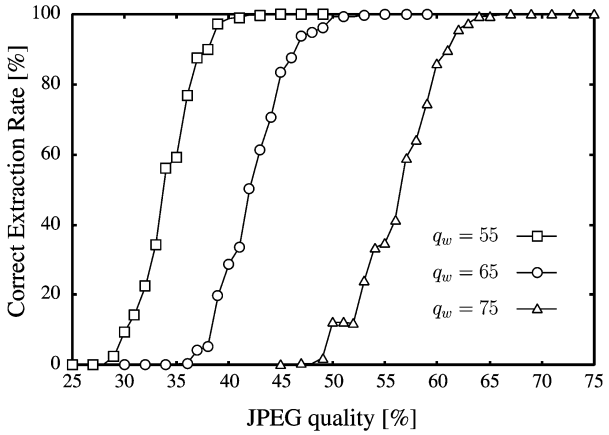

Fig. 8. Tolerance for JPEG compression.

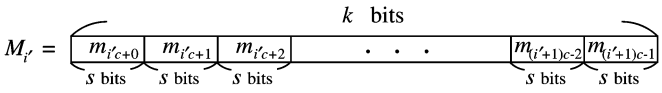

Fig. 9. Composition of the message $M_{i'}$.

public key k of Okamoto–Uchiyama encryption scheme. Since I_i and T are much smaller than $2^{k-1}(< p)$ 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^{k-1}.

Let m_i be

$$m_i = \begin{cases} I_i + Tw_j, & \text{marking position} \\ I_i, & \text{elsewhere} \end{cases} \tag{35}$$

and s be the maximum bit length of m_i. Since s is much smaller than k, the message can be replaced by

$$M_{i'} = \sum_{t=0}^{c-1} m_{i'c+t} 2^{st}, \quad 0 \le i' \le \frac{L}{c-1} \tag{36}$$

where

$$c = \left\lceil \frac{k}{s} \right\rceil. \tag{37}$$

It is illustrated in Fig. 9. If the ciphertext of the message $M_{i'}$ is calculated by $\mathcal{M}$ using com_j and I_i in our proposed fingerprinting protocol, the enciphering rate becomes at most 1/3 in theory.

In order to perform the above operations, the fingerprinting protocol of Steps 4 and 5 proposed in Section III is changed as follows.

[Modified Fingerprinting Protocol]

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

$$y_i = \begin{cases} g^{I_i} \cdot \mathrm{com}_j^T \bmod N, & \text{marking position} \\ g^{I_i} \bmod N, & \text{elsewhere.} \end{cases} \tag{38}$$

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

$$Y_{i'} = \left(\prod_t (y_{i'c+t})^{2^{st}} \right) \cdot h^{b_{i'}} \bmod N. \tag{39}$$

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

Remark 3: From (35)–(38) and the property P3, (39) is expressed by

$$\begin{aligned} Y_{i'} &= \left(\prod_t g^{m_{i'c+t} 2^{st}} \right) \cdot h^r \bmod N \\ &= g^{\sum m_{i'c+t} 2^{st}} h^r \bmod N \\ &= g^{M_{i'}} h^r \bmod N \\ &= E(M_{i'}, r). \end{aligned} \tag{40}$$

B. Security

On the security of the modified scheme, we only consider on Steps 4 and 5, as we have already discussed the other steps in Section III. First, we show the relation between $Y_{i'}$ and its data structure. If the Okamoto–Uchiyama encryption scheme is secure and the bit-length of $M_{i'}$ is less than k, $\mathcal{B}$ can decrypt $Y_{i'} = E(M_{i'}, r)$. Here, in (39) and (40), several pieces $m_{i'c+t}$ of fingerprinted images 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 (36). If $\mathcal{M}$ changes the data structure, $\mathcal{B}$ cannot decompose it into the correct pieces $m_{i'c+t}$, and then he can claim the fact. Hence, with the knowledge of data structure, $\mathcal{B}$ can decompose the decrypted message $M_{i'}$ into $m_{i'c+t}$, and finally get the fingerprinted image. Furthermore, as $M_{i'}$ is simply produced by composing several pieces of $m_{i'c+t}$, $\mathcal{B}$ cannot derive any information about original image from the decrypted message.

C. Comparison of the Enciphering Rate

In this section, we discuss the enciphering rate of our scheme compared with the conventional one. We assume that the size of $\mathcal{B}$'s 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 x bits. Then, the total amount of plain data of $\mathcal{M}$'s contents is xL. In the binary proof protocol, $\mathcal{B}$ sends com_j, $\widehat{\mathrm{com}}_j$, and $r_j, (0 \le j \le \ell - 1)$, so the amount of data transmitted between $\mathcal{B}$ and $\mathcal{M}$ is $5\ell \log_2 N$. The amount of data in [6] and [7] must be larger, because they use two commitment schemes and zero-knowledge proofs. As L will be much larger than ℓ, we evaluate the enciphering rate only by the encrypted and fingerprinted image.

In [6] and [7], the modulus is n which is composite of two large primes. Since only one bit information is encrypted if bit commitment is used, each bit of the frequency components must be encrypted; thus, the total amount of encrypted data is $xL \log_2 n$ bits. On the other hand, the modulus of our schemes is $N(= p^2 q, 3k$ bits). In the original scheme, the amount of encrypted data is $L \log_2 N (= 3kL)$ bits as each component is encrypted. In the modified scheme, it is $(L \log_2 N)/c (\simeq 3xL)$ bits, because, from (37), there are at most L/c messages $M_{i'}$ to be encrypted, since $s \simeq x$. Here, if $\log_2 n \simeq \log_2 N = 3k$, the enciphering information rates are indicated in Table II. Since

TABLE II
ENCIPHERING RATE

conventional	original	modified
$1/3k$	$x/3k$	$1/3$

the enciphering rate of Paillier cryptosystem is 1/2, our protocol can achieve the rate if the crytosystem is applied instead of Okamoto–Uchiyama encryption scheme.

Furthermore, the rate can be raised by restricting the embedding positions because of the following reason. In our proposed embedding operation, the high-frequency components should be avoided to embed a fingerprint, as such components are easily and seriously affected by attacks [1]. Here, if the high-frequency components are encoded by an arithmetic code to reduce the data length instead of encryption, the total amount of the data is decreased. Then, the tradeoff between the security and the rate should be considered, because if the number of the encrypted components is very few, $\mathcal{B}$ may be able to derive the selected position and remove or change the embedded fingerprint.

VII. CONCLUSION

We have proposed a new anonymous fingerprinting scheme based on the Okamoto–Uchiyama encryption scheme. The achievement of our proposed scheme is the improvement of enciphering rate that is too small to implement for any applications in the conventional ones, and we show a successful method for how to embed information in an image without the knowledge of the value. Using the Okamoto–Uchiyama encryption scheme, an encrypted fingerprint can be embedded in an encrypted image by customizing the quantized DCT coefficients, and the high enciphering rate is achieved by designing the message space of a ciphertext. As a result, the enciphering rate becomes, at most, 1/3 in theory for the Okamoto–Uchiyama scheme and 1/2 for Paillier cryptosystems; such rates are reasonable for cipher communication. Furthermore, the protocol is performed between only two parties, a buyer and a merchant, which is similar to a real-world market.

REFERENCES

[1] S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*. Norwood, MA: Artech House, 2000.

[2] N. R. Wagner, "Fingerprinting," in *Proc. IEEE Symp. Security and Privacy*, 1983, pp. 18–22.

[3] B. Pfitzmann and M. Schunter, "Asymmetric fingerprinting," in *Proc. Eurocrypt*, 1996, vol. 1070, pp. 84–95.

[4] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 643–649, May 2001.

[5] B. Pfitzmann and M. Waidner, "Anonymous fingerprinting," in *Proc. Eurocrypt*, vol. 1233, 1997, pp. 88–102.

[6] B. Pfitzmann and A. Sadeghi, "Coin-based anonymous fingerprinting," in *Proc. Eurocrypt*, 1999, vol. 1592, pp. 150–164.

[7] ——, "Anonymous fingerprinting with direct nonrepudiation," in *Proc. Asiacrypt*, vol. 1976, 2000, pp. 401–414.

[8] M. Kim, J. Kim, and K. Kim, "Anonymous fingerprinting as secure as the bilinear Diffie–Hellman assumption," in *Proc. ICICS*, vol. 2513, 2002, pp. 97–108.

[9] H. S. Ju, H. J. Kim, D. H. Lee, and J. I. Lim, "An anonymous buyer-seller watermarking protocol with anonymity control," in *Proc. ICICS*, vol. 2587, 2003, pp. 421–432.

[10] J. G. Choi, K. Sakurai, and J. H. Park, "Does it need trusted third party? design of buyer-seller watermarking protocol without trusted third party," in *Proc. ACNS*, vol. 2846, 2003, pp. 265–279.

[11] G. Brassard, D. Chaum, and C. Crepeau, "Minimum disclosure proofs of knowledge," *J. Comput. Syst. Sci.*, vol. 37, pp. 156–189, 1988.

[12] T. Okamoto and S. Uchiyama, "A new public-key cryptosystem as secure as factoring," in *Proc. Eurocrypt*, vol. 1403, 1998, pp. 308–318.

[13] M. Kuribayashi and H. Tanaka, "A new anonymous fingerprinting with high enciphering rate," in *Proc. Indocrypt*, vol. 2247, 2001, pp. 30–39.

[14] ——, "A watermarking scheme applicable for fingerprinting protocol," in *Proc. IWDW*, vol. 2939, 2004, pp. ,532–543.

[15] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[16] P. Paillier, "Public key cryptosystems based on degree residuosity classes," in *Proc. Eurocrypt*, vol. 1592, 1999, pp. 223–238.

[17] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 1897–1905, Nov. 1998.

[18] W. Trappe, M. Wu, Z. J. Wang, and K. J. R. Liu, "Anti-collusion fingerprinting for multimedia," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 1069–1087, Apr. 2003.

Minoru Kuribayashi (M'01) received the B.E., M.E., and D.E. degrees from Kobe University, Kobe, Japan, in 1999, 2001, and 2004, respectively.

Since 2002, he has been a Research Associate with the Department of Electrical and Electronics Engineering, Kobe University. His research interests are in digital watermarking, information security, and cryptography.

Hatsukazu Tanaka (F'01) received the B.E. degree from Kobe University, Kobe, Japan, in 1964, and the M.E. and D.E. degrees from Osaka University, Osaka, Japan, in 1966 and 1969, respectively.

He joined the Faculty of Engineering, University of Osaka Prefecture, in 1969. In 1973, he was appointed as an Associate Professor in the Department of Electrical Engineering, Kobe University. From 1988 to 2004, he was a Professor in the Department of Electrical and Electronics Engineering, Kobe University. Since 2005, he has been a Professor Emeritus of Kobe University and President of the Kobe Institute of Computing (Graduate School of Information Technology). From 1980 to 1981, he was a member of the Communication Group of the University of Toronto, Toronto, ON, Canada, as a Visiting Scientist. His main interests are in the basic theory of information engineering, such as information theory, coding theory, cryptography and information security, and image processing.

Dr. Tanaka is a Fellow of the IEICE and a member of IACR.