A New Anonymous Fingerprinting Scheme with High Enciphering Rate

Minoru Kuribayashi[1] and Hatsukazu Tanaka[2]

[1] Division of Information and Media Science
Graduate School of Science and Technology, Kobe University
1-1 Rokkodai-cho, Nada-ku, Kobe, Japan 657-8501
minoru@es3.eedept.kobe-u.ac.jp
[2] Department of Electrical and Electronics Engineering
Faculty of Engineering, Kobe University
1-1 Rokkodai-cho, Nada-ku, Kobe, Japan 657-8501
tanaka@eedept.kobe-u.ac.jp

Abstract. We propose a new anonymous fingerprinting scheme using Okamoto-Uchiyama cryptosystem[1]. In the previous schemes[2]-[4] the enciphering rate is so small that it seems very difficult to implement for any applications. In order to improve the rate, we have applied the Okamoto-Uchiyama cryptosystem for our fingerprinting protocol. As the results, a buyer can commit a fingerprint to a merchant being embedded in a digital content anonymously and efficiently, and then the amount of encrypted data is controlled in a reasonable size. The security can also be protected for both of a buyer and a merchant in our scheme.

1 Introduction

According to the development of the Internet, multi-media become to treat digital contents 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. Watermarking[5] 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, and the applications can be classified by a kind of embedded information as follows. When the information indicates a copyright owner, it can be 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. In the scheme an original merchant embeds the buyer's identity in his/her contents by himself/herself. Therefore, the merchant can not prove the buyer's treachery to anyone. To solve the problem, some cryptographic methods were applied for an asymmetric fingerprinting scheme[6]. Furthermore, an anonymous fingerprinting scheme[2] 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 [2] has been presented only a scheme using general theorems. The explicit construction was shown in [3] and [4] 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. If one uses the fingerprinting scheme for music, movie, etc., the amount of data to be sent will become incredibly large. Therefore, the problem is how to embed a fingerprint in the digital content efficiently.

In this paper we propose a new construction scheme of anonymous fingerprinting that overcomes the above drawback by exploiting Okamoto-Uchiyama cryptosystem[1]. Since it has a homomorphic property, the multiplication of encrypted fingerprint and digital content is equivalent to embed a fingerprint in the digital content. The property can make a merchant embed an buyer's identity information in the ciphertext of his/her contents. If the buyer can convince the merchant that the sent ciphertext really includes his/her identity, the anonymity of the buyer can be established. The trade between a buyer and a merchant is executed as follows. The buyer encrypts a fingerprint and commits it to the merchant using zero-knowledge proofs. The merchant embeds the received data in his/her encrypted digital content and returns it to the buyer. Finally the buyer decrypts and gets the fingerprinted content without disclosing the fingerprint to the merchant. As the results, only the buyer gets the fingerprinted content unless he/she redistributes it. Our main contribution is the achievement of a better enciphering rate than the conventional ones[2]-[4].

2 Preliminary

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 scheme are reviewed, and some inherent problems are disclosed. Finally the Okamoto-Uchiyama public-key cryptosystem is summarized in order to refer the encryption and decryption functions, and their properties.

2.1 Fingerprinting

Digital contents such as image, music, movie, 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 prevent 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/her a "traitor". The fingerprinting schemes can be classified into the following three classes.

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

Asymmetric: Fingerprinting is a interactive protocol between a buyer and a merchant. After the sale, only the buyer obtains the data with a fingerprint. If the merchant has found the fingerprinted copy somewhere, he/she can identify the traitor and prove to the third party.

Anonymous: A buyer can purchase a fingerprinted content without informing his/her identity to a merchant, but the merchant can identify the traitor later. It also retains the asymmetric property.

Pfitzmann et al.[2] has constructed an anonymous fingerprinting system by seven protocols; *Registration center key distribution, Registration, Data initialization, Fingerprinting, Identification, Enforced identification* and *Trail*. Our result is contributed to the *Fingerprinting* protocol, namely it is how to embed a fingerprint in a digital data anonymously at two-party protocol.

2.2 Bit Commitment Scheme

In the anonymous 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/her encrypted content. Finally, the buyer receives the encrypted and fingerprinted content and decrypts it. After the protocol, only the buyer gets the fingerprinted content without disclosing his/her identity. Here, one of the most important things is how to embed the encrypted fingerprint in the encrypted content. To accomplish it, Pfitzmann et al.[3][4] exploit two commitment schemes. One is applied for the verification that the commitment really includes the fingerprint to be embedded and the other is for the embedding of the fingerprint in the merchant's contents. The former is based on the discrete logarithm problem, and the latter is on the quadratic residues[7] of which security depends on the difficulty of factoring n. Though an encrypted fingerprint can be embedded in the encrypted content, the enciphering rate is very small because the commitment can contain only one-bit message in $\log n$-bit ciphertext. To improve the rate, we propose a new method based on the Okamoto-Uchiyama cryptosystem[1].

2.3 Okamoto-Uchiyama Cryptosystem

Let p and q be two large primes ($|p| = |q| = k$ bits) and $N = p^2q$. Choose $g \in (\mathbf{Z}/N\mathbf{Z})$ 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 $h = g^N \bmod N$ and a function $L(x) = (x-1)/p$. Here a public key is (N, g, h, k) and a secret key is (p, q).

The cryptosystem, based on the exponentiation mod$N$, is constructed as follows.

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

$$C = g^m h^r \pmod{N}. \tag{1}$$

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

$$m = \frac{L(C_p)}{L(g_p)} \pmod{p}, \tag{2}$$

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 a homomorphic property : if $m_0 + m_1 < p$,

$$E(m_0,\, r_0) \cdot E(m_1,\, r_1) = E(m_0 + m_1,\, r_0 + r_1) \pmod{N}. \tag{3}$$

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 $\mathbf{Z}/N\mathbf{Z}$.

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

The notation used here is applied for our proposed scheme in the following section.

3 Proposed Scheme I

The idea of our proposed scheme is to exploit the Okamoto-Uchiyama cryptosystem for anonymous fingerprinting. If we assume that a fingerprint is denoted by a number m_0 and a digital content is given by a number m_1, then a fingerprinted item becomes $m_0 + m_1$ from the property P1. In our scheme a buyer $\mathcal{B}$ can commit his/her identity to a merchant $\mathcal{M}$ as a fingerprint without informing the real value, and $\mathcal{M}$ can embed the fingerprint in the content at the enciphered form. After receiving the encrypted and fingerprinted content, $\mathcal{B}$ decrypts it, but can not remove the fingerprint.

3.1 Fingerprinting Protocol

The anonymous fingerprinting protocol is executed between a buyer $\mathcal{B}$ and a merchant $\mathcal{M}$. $\mathcal{B}$ commits his/her identity, $id = \sum w_j 2^j$ $(0 \le j \le \ell - 1)$ to $\mathcal{M}$ the enciphered form, com_j, and $\mathcal{M}$ encrypts his/her content 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 registration proof and his/her identity proof $W = g^{id} \bmod N$. Under the assumption, the fingerprinting protocol is given as follows.

[*Fingerprinting*]
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 to satisfy the following equation.

$$a = \sum_{j=0}^{\ell-1} a_j 2^j \tag{4}$$

A bit commitment of each w_j is calculated as

$$com_j = g^{w_j} h^{a_j} \pmod N, \tag{5}$$

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

$$V = h^a \pmod N, \tag{6}$$

and makes sure that the following equation can be satisfied.

$$\prod_j {com_j}^{2^j} \overset{?}{=} W \cdot V \pmod N \tag{7}$$

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

$$Y_i = \begin{cases} g^{I_i} h^{b_i} \cdot com_j^T \cdot g^{-\frac{T}{2}} \pmod N & \text{marking position} \\ g^{I_i} h^{b_i} \pmod N & \text{elsewhere} \end{cases} \tag{8}$$

and sends it to $\mathcal{B}$
Step 5. Since the received Y_i is rewritten as

$$Y_i = \begin{cases} g^{(I_i + Tw_j - \frac{T}{2})} h^{Ta_j + b_i} \pmod N & \text{marking position} \\ g^{I_i} h^{b_i} \pmod N & \text{elsewhere,} \end{cases} \tag{9}$$

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

$$D(Y_i) = \begin{cases} I_i + Tw_j - \frac{T}{2} \pmod p & \text{marking position} \\ I_i \pmod p & \text{elsewhere} \end{cases} \tag{10}$$

On the deciphered message, if $w_j = 1$, then $T/2$ has been added to I_i, and if $w_j = 0$, then $T/2$ has been subtracted from I_i. As the characteristic is suitable for several watermarking schemes like [8], our scheme can be applied easily.

Remark 1. If we regard w_j as a message and a_j as a random number, then com_j can be shown by $E(w_j, a_j)$ and com_j^T by $E(Tw_j, Ta_j)$ because

$$\begin{aligned} com_j^T &= (g^{w_j} h^{a_j})^T \pmod N \\ &= g^{Tw_j} h^{Ta_j} \pmod N \\ &= E(Tw_j, Ta_j). \end{aligned} \tag{11}$$

In Eq.(8), $g^{I_i} h^{b_i} g^{-T/2} = E(I_i - T/2,\, b_i)$ can be regarded as $\mathcal{M}$'s enciphered content, and then from the property P1 Y_i at the marking position can be rewritten as

$$\begin{aligned} Y_i &= E(Tw_j,\, Ta_j) \cdot E(I_i - \tfrac{T}{2},\, b_i) \\ &= E(I_i + Tw_j - \tfrac{T}{2},\, Ta_j + b_i) \end{aligned} \tag{12}$$

Here from the subsection 2.3, the message $I_i - T/2$ must satisfy an inequality $0 < I_i - T/2 < 2^{k-1}$. If $\mathcal{M}$ use I_i as a pixel value directly, the suitable pixel that satisfies the above inequality can be easily selected to embed a fingerprint. However, if $\mathcal{M}$ applies the transformed coefficients, the message should be modified for the adaptive data structure.

3.2 Security for the Merchant

In order to check the security, we consider some possible attacks. $\mathcal{B}$ may be able to forge his/her identity as he/she has not proved that the values w_j $(0 \leq j \leq \ell - 1)$ are binary in the fingerprinting protocol. To solve the problem, the following additional protocol should be performed.

[*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

$$Q_j = com_j^{t_j} \cdot g^{c_j} \pmod{N}, \tag{13}$$

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

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

$$D(Q_j) = w_j t_j + c_j \pmod{N} \tag{14}$$

and then he/she generates a random number r_j and calculates

$$\hat{com}_j = com_j^{t_j + c_j} \cdot h^{r_j} \pmod{N} \tag{15}$$

using the values c_j and Q_j or $t_j + c_j$. The detail is shown in the following Remark 2.

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

Step 4. If Eq.(13) is satisfied for the received t_j and c_j, $\mathcal{B}$ sends r_j to $\mathcal{M}$. If it is not satisfied, he/she can claim $\mathcal{M}$'s fraud.

Step 5. By verifying Eq.(15), $\mathcal{M}$ can certified that com_j contains only 1-bit information.

Remark 2. If $w_j = 0$ in the Step 2, then $D(Q_j) = c_j$ and $Q_j = g^{c_j} g^{a_j t_j} \bmod N$. Using Q_j and c_j, $\mathcal{B}$ can calculate

$$\begin{aligned} \hat{com}_j &= Q_j \cdot g^{-c_j} h^{a_j c_j + r_j} \pmod{N} \\ &= h^{a_j (t_j + c_j) + r_j} \pmod{N} \\ &= E\big(0,\, a_j(t_j + c_j) + r_j\big) \\ &= com_j^{t_j + c_j} \cdot h^{r_j} \end{aligned} \tag{16}$$

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

$$\begin{aligned} \hat{com}_j &= g^{t_j+c_j} h^{a_j(t_j+c_j)+r_j} \pmod N \\ &= E\big(t_j + c_j,\, a_j(t_j + c_j) + r_j\big) \\ &= com_j^{t_j+c_j} \cdot h^{r_j} \end{aligned} \tag{17}$$

Otherwise, $\mathcal{B}$ can not calculate $\hat{com}_j$ using the decrypted Q_j because the knowledge of each t_j and c_j or $t_j + c_j$ is inevitable. Therefore the lack of information makes it impossible to calculate $\hat{com}_j$ when w_j is not binary. From the above facts, the following lemma can be proved.

Lemma 1. *$\mathcal{B}$ can prove that w_j is binary using a zero-knowledge protocol.*

Proof. $\mathcal{B}$ can not obtain the values both t_j and c_j from Q_j, but only $w_j t_j + c_j$. Without the knowledge of the two values, $\mathcal{B}$ can not calculate $com_j^{t_j+c_j}$ except only two cases of $w_j = 0$ and $w_j = 1$. As $\mathcal{B}$ knows w_j, a_j and $w_j(t_j + c_j)$, $\hat{com}_j$ can be calculated by following Eqs.(16) and (17) if w_j is binary. It is remarkable that from the property P3 random number r_j changes the ciphertext $com_j^{t_j+c_j}$ to $com_j^{t_j+c_j} \cdot h_j^r = E\big(w_j(t_j + c_j),\, a_j(t_j + c_j) + r_j\big)$ preserving the plaintext $w_j(t_j + c_j)$. It guarantees that no information about w_j leaks to $\mathcal{M}$ as he/she can not distinguish $E\big(0,\, a_j(t_j + c_j) + r_j\big)$ and $E\big(t_j + c_j,\, a_j(t_j + c_j) + r_j\big)$. When $\mathcal{B}$ reveals r_j, $\mathcal{M}$ can make sure that w_j is binary by verifying Eq.(15), but can not get information anymore. Furthermore, $\mathcal{M}$ can not deceive $\mathcal{B}$ in the Step 2 as he/she should reveal the values t_j and c_j later to receive r_j. □

Using the above protocol, $\mathcal{B}$ can prove that w_j is binary from the Lemma 1 and hence $\mathcal{M}$ can embed $\mathcal{B}$'s identity properly and securely in his/her contents. Other possible attack is to remove or change the embedded his/her identity information directly from a fingerprinted content, but it is equivalent to attack the applied watermarking system. Then we can obtain the following theorem.

Theorem 1. *The security concerning to $\mathcal{M}$ is protected if the applied watermarking system is robust against attacks.*

3.3 Security for the Buyer

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

⟨**A1**⟩ The discrete logarithm problem is too difficult to solve.
⟨**A2**⟩ The Okamoto-Uchiyama cryptosystem is secure.
⟨**A3**⟩ $\mathcal{B}$ dose not redistribute a copy.

From these assumptions, the following theorem can be proved.

Theorem 2. *$\mathcal{B}$ can purchase contents 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, 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. From the property P2, $\mathcal{M}$ can not 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 can be extracted from the decrypted Y_i. However, $\mathcal{M}$ never get it under the assumption A3. Hence the anonymity of $\mathcal{B}$ is preserved. □

From the Theorem 2, $\mathcal{M}$ can not abuse the identity of $\mathcal{B}$. Therefore, the security concerning to $\mathcal{B}$ is protected.

4 Proposed Scheme II

4.1 Modified Fingerprinting Protocol

In the proposed scheme I, each I_i is encrypted and fingerprinted independently. Since I_i and T are much smaller than $2^{k-1}(< p)$ and the ciphertext is much larger than p, the enciphering rate is small. To improve the drawback, the size of message to be encrypted should be modified as large as 2^{k-1}. Let m_i be

$$m_i = \begin{cases} I_i + Tw_j - \frac{T}{2} & \text{marking position} \\ I_i & \text{elsewhere,} \end{cases} \tag{18}$$

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

$$M_{i'} = \sum_{t=0}^{c-1} m_{i'c+t} 2^{st}, \qquad 0 \le i' \le L/c - 1, \qquad c = \lceil k/s \rceil \tag{19}$$

After the modification, each $M_{i'}$ is encrypted to $E(M_{i'},\, r)$, where r is a random number. Let y_i be the encrypted and fingerprinted I_i. The fingerprinting protocol of Step 4 and Step 5 proposed in the previous section is changed as follows.

[*Fingerprinting(modified)*]
Step 4. In order to get the encrypted and fingerprinted content y_i, $\mathcal{M}$ calculates

$$y_i = \begin{cases} g^{I_i} \cdot com_j^T \cdot g^{-\frac{T}{2}} \pmod N & \text{marking position} \\ g^{I_i} \pmod N & \text{elsewhere} \end{cases} \tag{20}$$

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

$$Y_{i'} = \left(\prod_t (y_{i'c+t})^{2^{st}} \right) \cdot h^{b_{i'}} \pmod N \tag{21}$$

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

Remark 3. From Eqs.(11),(18)-(20) and the property P3, Eq.(21) can be expressed by

$$\begin{aligned} Y_{i'} &= \Big(\prod_t g^{m_{i'c+t}2^{st}}\Big) \cdot h^r \pmod N \\ &= g^{M_{i'}} h^r \pmod N \\ &= E(M_{i'},\, r). \end{aligned} \tag{22}$$

4.2 Security

On the security of the proposed scheme Ⅱ, we should consider only on Step 4 and Step 5 as we have already discussed the other steps in the previous section. First, we show the relation between $Y_{i'}$ and its data structure. If the Okamoto-Uchiyama cryptosystem 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 Eqs.(21) and (22) several pieces $m_{i'c+t}$ of fingerprinted content that compose $M_{i'}$ are encrypted in one ciphertext $E(M_{i'}, r)$, though each piece is encrypted in the proposed scheme I. Therefore, $M_{i'}$ should retain a special data structure described by Eq.(19). If $\mathcal{M}$ changes the data structure, $\mathcal{B}$ can not decompose it into the correct pieces $m_{i'c+t}$, and then he/she 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 content. Furthermore, as $M_{i'}$ is simply produced by composing several pieces of $m_{i'c+t}$, $\mathcal{B}$ can not derive any information about original content from the decrypted message.

5 Improvement of the Enciphering Rate

In this section, we discuss the efficiency of our scheme compared with the conventional one. Here, omitting the computational complexity, we only consider the enciphering rate, as every calculation is simple modular multiplication or exponentiation that is similar to the conventional one. We assume that a digital content consists of L pixels of x-bit scale image and $\mathcal{B}$'s identity is ℓ bits. As L is much larger than ℓ, we evaluate the rate only by the encrypted and fingerprinted content. In [3] and [4], the security is based on the difficulty of factoring n. When each bit of the content is encrypted, thus the total amount of encrypted data is $xL \log n$ bits. On the other hand, the security of our schemes is based on the difficulty of factoring $N(= p^2q,\ 3k$ bits). In the proposed scheme I, the amount of encrypted data is $L \log N(= 3kL)$ bits as each pixel is encrypted. In the proposed scheme Ⅱ, it is $(L \log N)/c\,(\simeq 3xL)$ bits, because there are L/c messages $M_{i'}$ to be encrypted, where s is the bit-length of each message and $s \simeq x$. Here, if $\log n \simeq \log N = 3k$, the enciphering information rates are indicated in Table 1.

Furthermore, the rate can be increased by restricting the embedding positions because of the following. Some watermarking schemes are designed to embed in the spatial domain, but almost all schemes in the transformed domain

Table 1. Enciphering rate

conventional	scheme I	scheme II
$1/3k$	$x/3k$	$1/3$

such as DCT, DFT, wavelet transform, etc. Generally, a signal embedded in the transformed (frequency) domain is more robust against attacks than in the spatial (time) domain, and the high frequency components are easily and seriously affected by attacks[5]. Hence, it is desirable to select some suitable components for embedding a fingerprint. Then, avoiding high frequency component to be encrypted, the total amount of the data can be decreased. However, 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. Therefore, the trade-off between the security and the rate should be considered.

6 Conclusion

We have proposed a new anonymous fingerprinting scheme based on the Okamoto-Uchiyama cryptosystem. The achievement of our proposed scheme is the improvement of enciphering rate that is too small in the conventional one. Using the Okamoto-Uchiyama cryptosystem, an encrypted fingerprint can be embedded in an encrypted content with high enciphering rate, and then the buyer's anonymity can be protected. Furthermore, the protocol can be performed between only two parties, a buyer and a merchant, which is similar to a real-world market.

References

1. T. Okamoto and S. Uchiyama, "A new public-key cryptosystem as secure as factoring," Proc. of EUROCRYPT'98, LNCS 1403, Springer-Verlag, pp.308-318, 1998.
2. B. Pfitzmann and M. Waidner, "Anonymous fingerprinting," Proc. of EUROCRYPT'97, LNCS 1233, Springer-Verlag, pp.88-102, 1997.
3. B. Pfitzmann and A. Sadeghi, "Coin-based anonymous fingerprinting," Proc. of EUROCRYPT'99, LNCS 1592, Springer-Verlag, pp.150-164, 1999.
4. B. Pfitzmann and A. Sadeghi, "Anonymous fingerprinting with direct non-repudiation," Proc. of ASIACRYPT'2000, LNCS 1976, Springer-Verlag, pp.401-414, 2000.
5. S. Katzenbeisser and F. A. P. Petitcolas, Information hiding techniques for steganography and digital watermarking, Artech house publishers, Jan. 2000.
6. B. Pfitzmann and M. Schunter, "Asymmetric fingerprinting," Proc. of EUROCRYPT'96, LNCS 1070, Springer-Verlag, pp.84-95, 1996.
7. G. Brassard, D. Chaum and C. Crepeau, "Minimum disclosure proofs of knowledge," Journal of Computer and System Sciences vol. 37, pp.156-189, 1988.
8. M. Kuribayashi and H. Tanaka, "A watermarking scheme based on the characteristic of addition among DCT coefficients," Proc. of ISW2000, LNCS 1975, Springer-Verlag, pp.1-14, 2000.