A Watermarking Scheme Applicable for Fingerprinting Protocol

Minoru Kuribayashi and Hatsukazu Tanaka

Department of Electrical and Electronics Engineering
Faculty of Engineering, Kobe University
1-1 Rokkodai-cho, Nada-ku, Kobe, Japan 657-8501
{minoru,tanaka}@eedept.kobe-u.ac.jp

Abstract. Fingerprinting protocol applies a watermarking technique to embed a fingerprinting information in a digital content such as music, image, movie, etc.. The cryptographic protocol is studied by many researchers, but how to apply watermarking techniques is not remarked. In this paper, we study the problem to implement the watermarking techniques in the fingerprinting protocol, and then propose an ingenious method to embed a fingerprinting information in a digital image. The alteration of the embedded information is difficult for a hostile buyer in our scheme.

1 Introduction

Fingerprinting is one of cryptographic techniques to protect the copyright of a valuable content. The idea is to embed tiny signals in the insignificant parts in order to keep an ownership information. So if an illegal user redistributes the fingerprinted content which contains his identity, he will be traced from the content by extracting the ownership information. In order to embed such information in the contents such as music, image, movie, etc. watermarking techniques[1] can be applied.

Fingerprinting protocol is basically performed by two parties, a buyer and a merchant. A buyer makes a trade with a merchant to get his content and then the merchant wants to prevent him from redistributing the content. In the cradle of the research, a symmetric scheme has been proposed, in which a merchant embeds a buyer's identity in his content by himself and sends it to him. However, in this scheme the merchant may frame the legal buyer because the merchant can distribute the fingerprinted content by himself as he has it, and then may insist that the distributed content is the same one sold to the buyer. So in order to protect the buyer's right, asymmetric schemes[2],[3] have been proposed in which the fingerprinted contents can be obtained only by a buyer. The fingerprinting information is encrypted before it is sent to a merchant and the encrypted information is embedded in the encrypted content by the merchant. Because the ciphertext can be decrypted only by the buyer, nobody can obtain the fingerprinted content except the buyer. Further, the anonymity of

the buyer can be achieved in [4],[5], and the enciphering rate has been improved in [6].

In order to embed a fingerprinting information in a content, a watermarking technique should be applied. However, in previous scheme[7] it is not deeply considered how to embed an encrypted information in an encrypted content and how to make the system robust against attacks. We study both fingerprinting and watermarking techniques and find the following difficulty to implement. In watermarking techniques for digital image, it is desirable to embed an information in the frequency components for both robustness and perceptual quality. However, as the frequency components are real number, there is a difficult problem to apply 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 or even number depending on the information bit. However, it seems difficult to exploit the method without the knowledge of an information bit.

In this paper, we propose a new watermarking scheme to embed an encrypted information in an encrypted contents. In order to apply a public-key cryptosystem, all frequency components of an image are quantized to integer. In the operation, a fingerprinting information is embedded to the quantized value. Here the degradation of the image should be considered. 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. As a quantization table used in the JPEG compression algorithm is designed considering human perceptual property, we modify the table so that it may be applicable for our embedding scheme. And in order to embed 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.

2 Preliminaries

2.1 Fingerprinting

Fingerprinting technique enable an author to embed an information about a buyer in his contents. If the buyer redistributes the copy, he is traced from the copy if the embedded information can be extracted correctly. Here, if the author can obtain the fingerprinted content at the end of the embedding protocol, it occurs a problem as follows. A dishonest author might try to distribute by himself the fingerprinted content, and claim that the innocent buyer redistributes the copy. Therefore, if the author can obtain the fingerprinted content after the protocol, he cannot prove to a third party that an illegal buyer redistributes the copy. In order to solve the problem, cryptographic techniques are applied. If an author embeds an encrypted information in an encrypted content and only the buyer can decrypts the ciphertext, only the buyer can obtain the fingerprinted content. Hence the author can accuse the illegal buyer.

2.2 Homomorphic Property

In our proposed fingerprinting protocol[6], the additive homomorphic property of Okamoto-Uchiyama encryption scheme[8] is applied to embed an encrypted fingerprint in an encrypted content. In the cryptosystem, the parameters are only integers.

Let $E(m, r)$ be an encryption function of a message m and a random number r. The modulus of the cryptosystem is $N = p^2q$, where p and q are large prime. If the function has the additive homomorphic property, the following equation can be satisfied.

$$E(m_1, r_1) \cdot E(m_2, r_2) = E(m_1 + m_2, r_1 + r_2) \pmod{N} \quad (1)$$

If we assume that a fingerprint is denoted by a number m_1 and a digital content is given by a number m_2, then a fingerprinted item becomes $m_1 + m_2$.

In public-key cryptosystems, several schemes retain a homomorphic property, but the above additive homomorphic property is for only a few schemes. In the schemes, Okamoto-Uchiyama scheme requires less computations and hence we adopt it. It can be replaced by Paillier cryptosystem[9] as it is excel at the enciphering rate and the structure is very similar to Okamoto-Uchiyama scheme except the modulus.

2.3 Fingerprinting Protocol

In a fingerprinting system, a merchant can embed an information related to a buyer in his contents such as music, picture, movie, etc. so as to trace the buyer later if he redistributes the copy. If a merchant embeds the information by himself and sells the fingerprinted content to a buyer, he may frame a legal buyer as a traitor. In the asymmetric scheme only a buyer can obtain the fingerprinted content after the fingerprinting protocol[2],[3]. In the protocol, first the buyer encrypts his identity information and sends it to the merchant. Then the merchant encrypts his content and embeds the buyer's identity information by multiplying the received ciphertext. Here, homomorphic property of the cryptosystem enable the merchant to embed the encrypted information into the encrypted content. Finally, the buyer receives the encrypted, fingerprinted ciphertext from the merchant and obtains the fingerprinted content by decryption using his secret key. This is illustrated in Fig.1. In detail, the asymmetric scheme has four protocols, key generation, fingerprinting, identification and dispute. The key generation protocol is a initial setting of the key parameters. And a merchant can identify the buyer from a illegal copy in the identification protocol and verify the fact in a dispute protocol. In the anonymous scheme, several protocols are added to the asymmetric scheme so as to guarantee the anonymity of the buyer. In the scheme a trusted third party ensures the registration of the buyer and hence the merchant can certify the anonymous buyer is a legal user of the system.

In [6] an anonymous fingerprinting protocol exploiting the additive homomorphic property of Okamoto-Uchiyama encryption scheme is proposed which

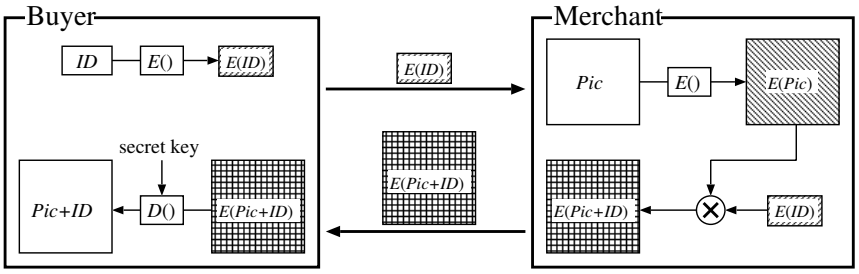

Fig. 1. Asymmetric fingerprinting protocol.

improves the enciphering rate dramatically. So the scheme seems to be realistic model to implement. Here we review the protocol briefly.

The fingerprinting protocol is executed between a buyer $\mathcal{B}$ and a merchant $\mathcal{M}$. We assume that the bit length of $\mathcal{B}$'s identity information is ℓ and $\mathcal{M}$'s digital content is composed of L pieces of components(for example, pixel in an image). $\mathcal{B}$ encrypts each bits of his/her identity, $id = \sum w_j 2^j$, $(0 \leq j \leq \ell - 1)$ and sends them to $\mathcal{M}$, and $\mathcal{M}$ encrypts each components of his/her content $I = \{I_i \mid 0 \leq i \leq L-1\}$ and multiplies each one to the received each ciphertexts respectively. We assume that $\mathcal{B}$ has already registered at a center $\mathcal{RC}$ and sent the proof $E(id, 0)$ to $\mathcal{M}$. The fingerprinting protocol is given as follows.

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.

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

Each identify information bit w_j is encrypted using the a_j as a random number, and the ciphertexts $E(w_j, a_j)$ are sent to $\mathcal{M}$.

Step 3. $\mathcal{M}$ verifies the validity of the received ciphertexts using a and $E(id, 0)$ by the following congruence.

$$\prod_j E(w_j, a_j)^{2^j} \equiv E(id, 0) \cdot E(0, a) \pmod{N} \tag{3}$$

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

$$Y_i = \begin{cases} E(I_i - T/2, b_i) \cdot E(w_j, a_j)^T \pmod{N} & \text{embedding position} \\ E(I_i, b_i) \pmod{N} & \text{elsewhere,} \end{cases} \tag{4}$$

and sends it to $\mathcal{B}$

Step 5. Since the received Y_i is rewritten as

$$Y_i = \begin{cases} E(I_i + Tw_j - \frac{T}{2}, Ta_j + b_i) \pmod N & \text{embedding position} \\ E(I_i, b_i) \pmod N & \text{elsewhere,} \end{cases} \tag{5}$$

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

$$\begin{cases} I_i + Tw_j - \frac{T}{2} \pmod p & \text{embedding position} \\ I_i \pmod p & \text{elsewhere} \end{cases}$$

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 [10], our scheme can be applied easily.

Remark 1. In Eq.(4) $E(w_j, a_j)^T$ can be shown by $E(Tw_j, Ta_j)$ because

$$\begin{aligned} E(w_j, a_j)^T &= E(w_j, a_j) \cdot E(w_j, a_j) \cdots E(w_j, a_j) \pmod N \\ &= E(\Sigma w_j, \Sigma a_j) \\ &= E(Tw_j, Ta_j). \end{aligned} \tag{6}$$

Therefore from the additive homomorphic property Y_i at the embedding position can be rewritten as

$$\begin{aligned} Y_i &= E(Tw_j, Ta_j) \cdot E(I_i - \tfrac{T}{2}, b_i) \\ &= E(I_i + Tw_j - \tfrac{T}{2}, Ta_j + b_i). \end{aligned} \tag{7}$$

2.4 Watermarking Technique

Watermarking is a technique to embed some information in digital contents without being perceived. The embedded information can be extracted from the watermarked contents using a secret key. There are two kinds of watermarking techniques to embed a watermark in an image. One exploits a spatial domain and the other a transformed domain using DCT, DFT, DWT, etc.. Generally a signal embedded in a transformed domain is robust against the signal processing which may be performed to remove the embedded signal[10].

"Requantization" is one of the popular techniques to embed a watermark in the transformed domain. First, an image is transformed to the frequency domain and then the components in the embedding position are quantized by a quantizing step size Q. The embedding procedure is given as follows(see Fig.2).

Step.1 An image is divided into smaller blocks, and each block is transformed to the frequency domain.

Step.2 A frequency component $f_{x,y}$ in the embedding position is quantized by a quantizing step size Q.

$$\hat{f}_{x,y} = int\big(f_{x,y}/Q\big) \tag{8}$$

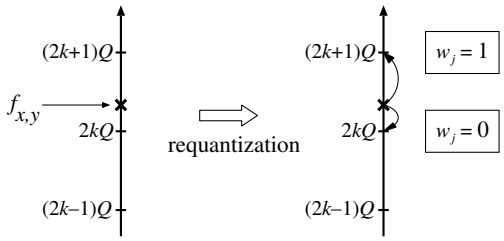

Fig. 2. Requantization procedure.

Step.3 A watermarking information bit w_t is embedded by the following equation.

$$\hat{f}'_{x,y} = \begin{cases} \hat{f}_{x,y} + 1 & w_t \neq \hat{f}_{x,y} \bmod 2 \\ \hat{f}_{x,y} & \text{otherwise} \end{cases} \tag{9}$$

Step.4 $\hat{f}'_{x,y}$ is multiplied by Q, and the watermarked frequency domain is transformed inversely to obtain a watermarked image.

In the extraction procedure, Step.1 and Step.2 of the above procedure are executed. Then the watermarked information bit is determined being based on whether the value of a quantized frequency component is odd or even.

In the fingerprinting techniques, it is desirable that a lot of information can be embedded in a content. In the conventional schemes[2]-[4] the "patchwork" method[11] has been used. The scheme can be easily applied for the fingerprinting schemes, but the amount of embedded information is too small to use. So in our proposed scheme, the requantization scheme is applied in order to embed a lot of information in a image.

3 How to Embed an Encrypted Information

3.1 Basic Idea

In order to embed an encrypted fingerprinting information bit in an encrypted content, the additive homomorphic property of public-key cryptosystem is applied. In a fingerprinting protocol, the operation is performed by Eq.(4). However, such public-key cryptosystem cannot use real value. Hence watermarking schemes exploiting 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. Then the fingerprinting information bit is embedded using the watermarking technique proposed in the previous section.

In the quantization process, if the frequency coefficients are quantized uniformly, it causes serious degradation of the image. So it should be quantized based on the human perceptual characteristic. And there is a serious problem in the embedding process. In the asymmetric and anonymous fingerprinting, a

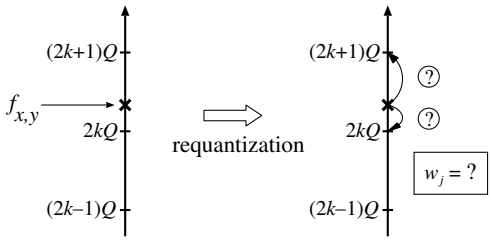

Fig. 3. Problem to embed an encrypted fingerprinting information.

merchant $\mathcal{M}$ cannot get a buyer $\mathcal{B}$'s plain identity information unless $\mathcal{B}$ shows it because the identity information is encrypted and then embedded in $\mathcal{M}$'s contents by multiplying ciphertexts. In such a situation, it seems to be impossible that $\mathcal{M}$ embeds $\mathcal{B}$'s identity information bits in his/her content using the watermarking technique without knowing the plaintext itself. Because a coefficient is quantized to the nearest even number if the bit is zero, otherwise to the odd number. Without the knowledge of the embedding information bit, such procedure cannot performed. It is shown in Fig.3.

In order to embed an information bit w_j without knowing the plaintext, the frequency coefficients of the embedding positions is first quantized to the nearest even number in our scheme. After the frequency coefficients are quantized to the even number, the following equation is calculated to embed the information bit.

$$E(\hat{f}_{x,y}, b_i) \cdot E(w_j, a_j) = E(\hat{f}_{x,y} + w_j, b_i + a_j) \pmod{N} \tag{10}$$

In this case, the quantized frequency coefficient becomes odd number if $w_j = 1$, otherwise even number. So even if the plain information bit is kept secret using cryptographic technique, it can be embedded in the frequency coefficient of a content. Here, the original value $f_{x,y}$ of the frequency coefficient should be considered as the following reason. If $f_{x,y}$ is less than the quantized coefficients, then $\hat{f}_{x,y} + w_j$ is not the nearest odd number and hence the degradation of the image is increased. Therefore Eq.(10) should be changed in such a case as follows.

$$E(\hat{f}_{x,y}, b_i) \cdot E(w_j, a_j)^{-1} = E(\hat{f}_{x,y} - w_j, b_i + a_j) \pmod{N} \tag{11}$$

Depending on $f_{x,y}$, one of the above two equation is selected to embed an encrypted and fingerprinting information bit.

3.2 Embedding Procedure

In a fingerprinting protocol, a buyer $\mathcal{B}$ encrypts his fingerprinting information bits w_j, and their ciphertexts $E(w_j, a_j)$ are sent to a merchant $\mathcal{M}$. First $\mathcal{M}$ performs DCT to the divided blocks of his content and then encrypts each quantized

DCT coefficient. Finally the encrypted and fingerprinted content is calculated by multiplying the received $E(w_j, a_j)$ to the encrypted coefficients at the embedding positions. Here, the embedding positions are determined by $\mathcal{M}$'s secret key and hence intentional alteration of the embedded information bit is difficult for $\mathcal{B}$.

The embedding procedure of proposed method is summarized in the followings.

[Buyer:]

Each fingerprinting information bit w_j is encrypted and the ciphertext $E(w_j, a_j)$ is sent to $\mathcal{M}$.

[Merchant:]

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

Step.2 Each DCT coefficient $f_{x,y}$ of each block is quantized to the nearest integer using a quantizing step size $Q_{x,y}$. Here the coefficients in the embedding positions are quantized to the nearest even number.

Step.3 Each quantized coefficient $\hat{f}_{x,y}$ is encrypted using the $\mathcal{B}$'s public key.

Step.4 Using the $\mathcal{M}$'s secret key the embedding coefficients are specified, and each fingerprinting information bit is embedded by multiplying two ciphertexts as follows

- If $f_{x,y} > \hat{f}_{x,y} Q_{x,y}$, then $E(w_j, a_j)$ is multiplied to the ciphertext of $\hat{f}_{x,y}$, which can be calculated by Eq.(10).
- else if $f_{x,y} \leq \hat{f}_{x,y} Q_{x,y}$, then $E(w_j, a_j)^{-1}$ is multiplied to the ciphertext of $\hat{f}_{x,y}$, which can be calculated by Eq.(11).

Step.4 The ciphertexts of fingerprinted content are sent to $\mathcal{B}$.

[Buyer:]

Step.1 The received ciphertexts are decrypted and the quantized DCT coefficients are recovered.

Step.2 Each quantizing step size $Q_{x,y}$ is multiplied to the corresponding quantized coefficient.

Step.3 By performing IDCT, the fingerprinted content can be obtained.

When $\mathcal{B}$ recovers the fingerprinted content, $Q_{x,y}$ used to quantize the original DCT coefficients is inevitable to recover the proper DCT coefficients. So we assume that they are shared previously between the buyer and the merchant.

In order to increase the robustness against attack, the embedding positions should not be selected from high frequency coefficients as 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 operation is repeatedly performed α times for different low frequency coefficients of several blocks.

Table 1. Quantization table of 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

3.3 Quantization Table

When a fingerprinting information 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 should be 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 1 is used. The table is designed to keep the perceptual quality as good as possible. So the table is suitable for quantization of an image. However, the table size is 8×8, and hence it is too small to keep the security of the information embedded in the block for the attack using the common signal processing. 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.

$$b_{x,y} = \begin{cases} q_{x,y/2} & (y=0,\ 2,\ 4,\ \ldots,\ 14) \\ \big(q_{x,y/2} + q_{x,y/2+1}\big)/2 & (y=1,\ 3,\ 5,\ \ldots,\ 13) \\ q_{x,7} & (y=15) \end{cases} \tag{12}$$

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

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

Where the fraction value is rounded cutoff method.

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

$$Q'_{x,y} = \frac{(100-q)}{50} Q_{x,y} \tag{14}$$

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

3.4 Extraction

Since the fingerprinting information is embedded by quantizing the DCT coefficients even/odd number, such information can be 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, it is transformed by DCT after partitioned into blocks. And then each coefficient in the embedding position is quantized using the corresponding $Q_{x,y}$. 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 can be determined by the sum of those amount. Here, the 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 round 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 the such extraction procedure.

4 Security

In this section, we consider the security of our proposed system. Here we assume the applied public-key cryptosystem is secure. Everyone can make a ciphertext of any message using the public key of a buyer, but no one can decrypt the ciphertext except the buyer who has the secret key. So the merchant cannot get the fingerprinting information from the received ciphertexts $E(w_j, a_j)$ directly. If the buyer redistributes a illegal copy and the embedded information is extracted from it, the merchant can obtain the fingerprinting information and hence trace the illegal buyer. The above discussion is described in [6].

Considering the robustness against common signal processing, one bit 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, which distributes randomly. Such DCT coefficients in the embedding positions are quantized to the nearest even number and a information bit is embedded using Eqs.(10) or (11). So the quantized value of DCT coefficients can be 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 degradation. Further, as the number of DCT coefficients are much larger than that of information bits, 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 fingerprinting information, which makes the coefficients randomly distributed. Several buyers may collude to analyze the embedding position by taking the difference of each fingerprinted content. But such attack can be avoided using the collusion secure code[12]. As the consequence, our proposed scheme is secure against intentional alteration of a hostile buyer.

5 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 cryptosystem, and it has already proved in [6]. 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 "Lana" that has 256 level gray scale with size of 256×256. Considering the robustness against signal processing attack, the size of α should be large. However, if α is increased, an hostile user may be able to deter the embedding positions and change the values. Because the candidates for the embedding positions are decreased. Hence considering the trade-off, we set $\alpha = 75$ in the following simulations.

If the quality factor q is decreased, the perceptual quality is decreased accordingly. Figure 4 shows the relation between q and PSNR. The robustness against attack can be increased if q is decreased, but the perceptual quality is decreased. Therefore there is a trade-off between the robustness and perceptual quality and it should be considered to apply our scheme. From our experiment, the value of q should is between 85 and 95.

The robustness against JPEG compression is examined and the results are shown in Fig. 5. From the results, the tolerance for JPEG compression is dependent on the value of q. Such value should be selected for the applied system. Concerning to the robustness against Gaussian filtering, the embedded information can be extracted without any errors.

6 Conclusion

We have proposed a watermarking scheme to embed an encrypted information in an encrypted content. In the conventional schemes, the protocol has been achieved by applying the additive homomorphic property, but their schemes do not mention how to use watermarking techniques. In this paper, we make clear how to embed an information keeping the true value secret, and how to use real value for a public-key cryptosystem using the quantization operation of

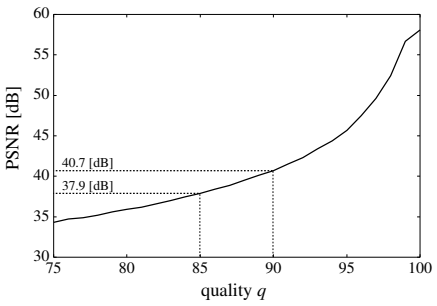

Fig. 4. PSNR versus quality q ($\alpha = 75$).

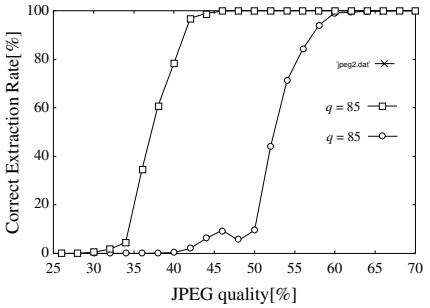

Fig. 5. Tolerance for JPEG Compression.

DCT coefficients. Before embedding an information bit, all DCT coefficients are quantized. Then the coefficients in the embedding positions are quantized even number before embedding. Then to keep the image quality as good as possible, the quantization table of JPEG algorithm is modified to reconstruct a suitable table for our proposed scheme from a point of human perceptual property.

References

1. S. Katzenbeisser and F. A. P. Petitcolas, *Information hiding techniques for steganography and digital watermarking.* Artech house publishers, Jan. 2000.
2. B. Pfitzmann and M. Schunter, "Asymmetric fingerprinting," *Proc. of EUROCRYPT'96*, LNCS 1070, Springer-Verlag, pp.84-95, 1996.
3. B. Pfitzmann and M. Waidner, "Anonymous fingerprinting," *Proc. of EUROCRYPT'97*, LNCS 1233, Springer-Verlag, pp.88-102, 1997.
4. B. Pfitzmann and A. Sadeghi, "Coin-based anonymous fingerprinting," *Proc. of EUROCRYPT'99*, LNCS 1592, Springer-Verlag, pp.150-164, 1999.
5. B. Pfitzmann and A. Sadeghi, "Anonymous fingerprinting with direct nonrepudiation," *Proc. of ASIACRYPT'2000*, LNCS 1976, Springer-Verlag, pp.401-414, 2000.
6. M. Kuribayashi and H. Tanaka, "A new anonymous fingerprinting with high enciphering rate," *Proc. of INDOCRYPT2001*, LNCS 2247, Springer-Verlag, pp.30-39, 2001.
7. N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE trans. on Image Process.*, vol. 10, no. 4, pp.643-649, 2001.
8. 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.
9. P. Paillier, "Public key cryptosystems based on degree residuosity classes," *Proc. of Eurocrypt'99*, LNCS 1592, Springer-Verlag, pp.223-238, 1999.
10. 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.
11. W. Bender, D. Gruhl and N. Morimoto, "Techniques for Data Hiding," *Proc. of SPIE*, pp.164-173, 1995.
12. D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE* Trans. Inform. Theory, vol.44, no.5, pp.1897-1905, 1998.