ON THE IMPLEMENTATION OF ASYMMETRIC FINGERPRINTING PROTOCOL

Minoru Kuribayashi, and Masakatu Morii

Graduate School of Engineering, Kobe University
1-1, Rokkodai, Nada, Kobe, Hyogo, Japan
email: kminoru@kobe-u.ac.jp

ABSTRACT

Digital fingerprinting of multimedia contents involves the generation of a fingerprint, the embedding operation, and the realization of traceability from redistributed contents. Considering a buyer's right, the asymmetric property in the transaction between a buyer and a seller must be achieved using a cryptographic protocol. In the conventional schemes, the implementation of a watermarking algorithm into the cryptographic protocol is not deeply discussed. In this paper, we propose the method for implementing the spread spectrum watermarking technique in the fingerprinting protocol based on the homomorphic encryption scheme, and evaluate the performance by simulation.

1. INTRODUCTION

Due to the recent advance in wide-band network and multimedia technologies, the distribution and share of digital multimedia contents are increasing. It also helps a malicious party to duplicate and redistribute the contents, hence the protection of the ownership is strongly required. Encryption of the content cannot solve the problem because it must be ultimately decrypted at legitimate users who are the potential traitors in a future. Therefore, additional protection mechanisms are needed to discourage unauthorized redistribution. One of the mechanisms is the fingerprinting of multimedia which enables a seller to trace illegal users by embedding identification information into the content prior to distribution [1].

The research on fingerprinting techniques is classified into two studies; collusion resistant fingerprinting systems and cryptographic protocol. Since each user purchases a content containing his own fingerprint, each content is slightly different. If users collect some of them, they try to find the difference and delete/change the embedded information. In order to tolerate such an attack, designing collusion resistant fingerprint codes [2, 3] and orthogonal fingerprinting schemes like the spread spectrum watermarking technique [4] had been proposed. In a cryptographic protocol, the goal is to achieve the asymmetric property between a buyer and a seller such that only the buyer can obtain an uniquely fingerprinted content because of the threat of dispute. If both of the party know the content, the buyer may redistribute a pirated copy but later repudiate it by insisting that the copy come from the seller. In [5, 6, 7], the asymmetric protocol is performed by exploiting the homomorphic property of the public-key cryptosystem that enables a seller to obtain the ciphertext of fingerprinted content by operating an encrypted fingerprint with an encrypted content. Since the ciphertext is computed using a buyer's encryption key, only the buyer can decrypt it; hence, only he can obtain the fingerprinted content. It is also desirable for the fingerprinting protocol to solve the unbinding problem such that the relation between fingerprint information and a specific transaction performed by a buyer and a seller [8]. Although the homomorphic property is effective for constructing asymmetric fingerprinting, there are problems in its implementation.

In this paper, we propose the method for implementing the spread spectrum watermarking technique by carefully designing parameters for rounding operation. If frequency components of digital contents are used for the embedding fingerprint information, they must be quantized in order to truncate real value to integer. Then, the precision of the frequency components should be considered in order not to degrade a watermarked image. When the spread spectrum watermarking technique in [4] is applied, the precision of the representing watermark signal is sensitive for the implementation. By scaling up the parameters by multiplying a constant factor, the precision is increased in our scheme. Then, the trade-off between the scaling factor and the amount of data to be transmitted must be considered. In addition, for the characteristic of the fingerprinting protocol, frequency components and the watermark signal must be separately encrypted after quantization. In such a case, the consistency of the precision is a sensitive issue. Since an embedding operation is performed by addition of frequency components and a spread spectrum sequence, the additive homomorphic property of public-key cryptosytems [9, 10] can be directly exploited for the embedding. Then, the separate rounding operation causes interference term in a deciphered data at a buyer side. Without loss of secrecy of an original content, the interference term is removed after decryption. The performance of our proposed method is evaluated comparing with the conventional scheme [4], which confirms the similar identification capability of illegal buyers.

2. RELATED WORKS

2.1 Asymmetric Property

If both a buyer and a seller obtain a fingerprinted content in a fingerprinting protocol, the seller cannot prove to a third party about the illegal distribution by the buyer, even if the buyer's fingerprint is extracted. This is because the seller may distribute it himself in order to frame an innocent buyer. Hence, it is desirable that only a buyer is able to obtain his own fingerprinted content in the protocol. Such a protocol is called asymmetric fingerprinting protocol. In order to achieve such an asymmetric property, the homomorphic property of public-key cryptosystems is introduced in the fingerprinting protocols [5, 6, 7].

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

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

where $g(\cdot)$ and $f(\cdot)$ is one of the operations, *addition, multiplication, XOR,* etc., which is related to the applied cryptosystem and the embedding algorithm (Most public-key cryptosystems select multiplication for $g(\cdot)$). If m_1 is regarded as a digital content and m_2 as a fingerprint, the fingerprint can be embedded in the content without decryption by multiplying those ciphertexts. Since these are calculated using buyer's public encryption-key, the fingerprinted content is decrypted only by the buyer, hence the asymmetric property is satisfied. The embedding operation based on the homomorphic property is basically performed for each element of fingerprint information which will be composed of bit-sequence or spread spectrum sequence, hence each element is separately embedded in its corresponding position. Thus, m_1 is not the entire content, but one of the components like the frequency elements to be fingerprinted by a watermarking technique.

In watermarking techniques [1] for digital images, it is advisable to embed information in the frequency components for both the robustness and perceptual quality. However, as the frequency components are generally represented by real value, there is a difficult problem to apply cryptographic techniques directly because they are based on the algebraic property of integer. Many schemes [6, 8] ignored the implementation of watermarking algorithm into the asymmetric fingerprinting protocols, instead they merely showed the validity of the cryptographic protocols which ensure the asymmetric property and the anonymity of buyers.

Considering the adaption of watermarking techniques for cryptographic fingerprinting protocol, a quantization method is useful as a fingerprint can be embedded when the coefficients are quantized. In [7], the quantization index modulation based watermarking technique (QIM) [11] is applied for the embedding procedure because it rounds the values of frequency components in integers. Prins et al. [12] adapted three kinds of dithering modulations, which can improve the robustness of the QIM method, to the fingerprinting scheme, and implemented the method using a sufficiently large scaling factor. However, the enciphering rate is neglected. We assume that the bit-length of the message space is ℓ_M and that of each watermarked frequency components is ℓ_m. Generally, ℓ_M is much larger than ℓ_m. In order to exploit the message space effectively, dozens of watermarked frequency components are packed in one message in [7], hence, the enciphering rate is almost equivalent to that of an applied cryptosystem by suitably designing the message space of a ciphertext. It is remarkable that a negative number must be avoided because it is represented by much longer bit-sequence under the finite field of applied cryptosystem, which affects the other packed ones.

Although the capacity of embeddable information is large, considering the robustness against collusion attacks the spread spectrum watermarking technique is superior to QIM and its variants. In [6], the adaption of Cox's spread spectrum watermarking scheme [4] is discussed. Regretfully, there is a problem in the implementation because the rounding-off operation is not deeply considered for the spread spectrum watermarking algorithm.

2.2 Collusion Resilience

It is important to generate fingerprints that can not only identify the colluders, but also resilient against the collusion attack. In a fingerprinting scheme, each watermarked copy is slightly different, hence, malicious users will collect c copies with respective watermark $W_t, (1 \leq t \leq c)$ in order to remove/alter the watermark. A number of works on designing fingerprints that are resistant against the collusion attack have been proposed. Many of them can be categorized into two approaches. One is to exploit the Spread Spectrum (SS) technique [4, 13, 14], and the other approach is to devise an exclusive code, known as collusion-secure code [2, 3, 15], which has traceability of colluders.

On the former approach, spread spectrum sequences which follow a normal distribution are assigned to users as fingerprints. The origin of the spread spectrum watermarking scheme is Cox's method [4] that embeds the sequence into frequency components of digital image and detects it using a correlator. Since normally distributed values allow the theoretical and statistical analysis of the method, modeling of a variety of attacks have been studied. Studies in [13] have shown that a number of nonlinear collusions such as interleaving attack can be well approximated by averaging collusion plus additive noise. So far, many variants of the spread spectrum watermarking scheme are based on the Cox's method.

Since the QIM watermarking technique [7] and its variants [12] are aiming at the extraction of a watermark bit-sequence, the latter approach is suitable to implement. The practicality of the latter approach is, however, restricted because of the long code length. Moreover, in [16], the traceability is further improved by combining a spread spectrum embedding like Cox's method. Hereafter, we focus on the implementation of Cox's method in a fingerprinting protocol.

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

$$x_i' = x_i(1 + \alpha w_i), \tag{2}$$

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

$$\mathsf{sim}(W, \tilde{W}) = \frac{W \cdot \tilde{W}}{\sqrt{\tilde{W} \cdot \tilde{W}}}, \tag{3}$$

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

At the detection, DCT coefficients of test image are subtracted from those of original image, and then the correlations with every candidates of watermark signal are computed. Thus, non-blind and informed watermarking scheme can be applied. In fingerprinting techniques, the original content may be available at a detection because a seller is assumed an author, or a sales agent who knows it.

A simple, yet effective collusion attack is to average some variants of copy because when c copies are averaged, the similarity value calculated by Eq. (3) results in shrinking by a factor of c, which will be roughly $\sqrt{L}/c$ [4]. Even in this case, we can detect the embedded watermark and identify the colluders by using an appropriately designed threshold.

2.3 Unbinding Problem

In the elementary fingerprinting protocol [6], fingerprint information to be embedded is not well considered, which is merely related to user's information such as name, address, phone number, e-mail address, etc.. When a seller finds an illegal copy and detects the corresponding buyer by extracting the fingerprint, he will go to court with the collected proofs. A malicious seller, however, frames the detected buyer by embedding the obtained fingerprint into the other contents which are more expensive than the detected one what he really sold to the buyer. Therefore, once a seller obtains a fingerprint, it is possible for him to transplant it into another much expensive contents so that he can get compensated more.

In [8], a fingerprint is binded with a common agreement (ARG) by producing the signature of a trusted watermark certification authority (WCA), and the transaction of digital contents is uniquely associated with a log file. For anonymity of buyers, a digital certification authority (CA) is introduced in the fingerprinting protocol. A buyer B first randomly selects a key pair (pk, sk) and send pk, which is pseudonym associated with B, to CA in order to get an anonymous certificate $Cert_{\mathtt{CA}}(pk)$. When B makes an order to a seller S, he checks the validity of $Cert_{\mathtt{CA}}(pk)$. Then S asks WCA to generate an unique watermark W for the current transaction between B and S. The detail is referred to [8].

3. IMPLEMENTATION FOR WATERMARKING ALGORITHM

In this section, we show how to implement the spread spectrum watermarking technique [4] in the fingerprinting protocol based on the homomorphic property of public-key cryptosystem.

The embedding operation in Eq.(2) can be easily performed using the additive homomorphic property of public-key cryptosystems such as Okamoto-Uchiyama encryption scheme [9] and Paillier cryptosystem [10]. Remember that Eq.(2) is composed of two operations; multiplication and addition for $g(\cdot)$ and $f(\cdot)$, respectively. Since the multiplication is realized by the iteration of addition, the embedding operation is represented by the multiplication and exponentiation as follows.

$$E_{pk}\big(x_i(1+\alpha w_i)\big) = E_{pk}(x_i)\cdot E_{pk}(w_i)^{\alpha x_i}, \tag{4}$$

where $E_{pk}(\cdot)$ is an enciphering function using a public key pk. Here, it is noticed that a watermark signal and DCT coefficients are generally represented by real value and they must be rounded to integer before the encryption. If such parameters are directly rounded to the nearest integers, it may result in the loss of information. Hence, they should be scaled before rounding-off. In addition, negative number should be avoided considering the property of a cryptosystem as mentioned in subsection 2.1. Hence, a rounding operation that maps real value into positive integer is required.

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

$$\overline{w}_i = int\big(s_w(w_i + p_w)\big), \tag{5}$$

where $int(a)$ outputs the nearest integer from a real value a. After the operation, WCA encrypts $\overline{w}_i$ using a public key pk, and the ciphertexts $E_{pk}(\overline{w}_i)$, p_w and s_w are sent to S.

Next, S performs the rounding operation to DCT coefficients $x_i, (1 \le i \le L)$ as follows. A constant value p_x is added to each DCT coefficient, and then scaled by $s_w s_x$. By quantizing it, the rounded DCT coefficient $\overline{x}_i$ is obtained.

$$\overline{x}_i = int\big(s_w s_x(x_i + p_x)\big) \tag{6}$$

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

$$\overline{\alpha}_i = int\big(s_x \alpha |x_i|\big). \tag{7}$$

Using the above items, S embeds $\overline{w}_i$ into $\overline{x}_i$ based on the additive homomorphic property of public cryptosystem as follows.

$$E_{pk}(\overline{x}_i)\cdot E_{pk}(\overline{w}_i)^{\overline{\alpha}_i} = E_{pk}(\overline{x}_i + \overline{\alpha}_i\overline{w}_i) \tag{8}$$

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

$$\begin{aligned} \overline{x}_i + \overline{\alpha}_i\overline{w}_i &= s_w s_x(x_i + p_x) + s_x\alpha|x_i|s_w(w_i + p_w), && (9)\\ &= s_w s_x\big((x_i + \alpha w_i|x_i|) + (p_x + \alpha|x_i|p_w)\big), && (10) \end{aligned}$$

the scaling factor $s = s_w s_x$ and the adjustment factor $p = (p_x + \alpha|x_i|p_w)$ are necessary to calculate the actual watermarked DCT coefficients $x_i + \alpha w_i|x_i|$. Therefore, these two parameters s and p are sent to B as well as $E_{pk}(\overline{x}_i + \overline{\alpha}_i\overline{w}_i)$.

After the decryption of the ciphertext $E_{pk}(\overline{x}_i + \overline{\alpha}_i\overline{w}_i)$, B divides the result by a factor of s, and then subtracts p;

$$\frac{D_{sk}\big(E_{pk}(\overline{x}_i + \overline{\alpha}_i\overline{w}_i)\big)}{s} - p = x_i + \alpha w_i|x_i|, \tag{11}$$

where $D_{sk}(\cdot)$ is a deciphering function using a secret key sk.

In Eq.(2), the watermarked coefficient x'_i is composed of two terms; x_i and $\alpha w_i x_i$. Since w_i is encrypted at the center WCA prior to the embedding operation at S, x_i and w_i are rounded separately. Considering the post-processing at B, the scaling factors s_w, s_x, and the compensation factor p should be constant. Here, we assume that a constant value is uniformly added to real values which are w_i and x_i to make it positive. Then, B must subtract the interference term related to both x_i and w_i, which requires additional communication costs. If the adjustment factor p is variable with respect to x_i, the amount of information to be sent to B from S becomes very large. In order to avoid it, we set p a constant value by controlling the value p_x. Even if p and α is known, to obtain x_i is still difficult, hence the secrecy of the original DCT coefficients is assured.

Notice that if the size of scaling factors s_w, s_x is increased, the proposed scheme can simulate the original Cox's method more precisely. From the viewpoint of enciphering rate, however, these factors should be small. Referring to [7], the bit-length of a watermarked coefficient $\overline{x}'_i = \overline{x}_i + \overline{\alpha}_i\overline{w}_i$, which is represented by a constant bit-length, is much smaller than that of message space in cryptosystems such as Okamoto-Uchiyama encryption scheme [9] and Paillier cryptosystem [10], and some of $\overline{x}'_i$ are packed in one message $\overline{M}$;

$$\overline{M} = \overline{x}'_i||\overline{x}'_{i+1}||\cdots||\overline{x}'_{i+n-1}, \tag{12}$$

Table 1: Conditions of simulation.

L	1000
α	0.1
p_w	10
p_x	5000
PSNR	34.93 [dB]

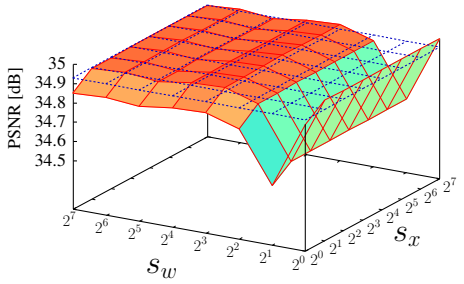

Figure 1: The comparison of the image quality.

where n is the number of packed coefficients and is dependent on s_w and s_x. The appropriate size of s_w and s_x are explored by implementing on a computer and evaluating the simulated performance. It is worth mentioning that the enciphering rate of Paillier cryptosystem approaches asymptotically 1 using the extension of the cryptosystem [17] and then more data can be packed in one ciphertext. Although the works in [18, 19] can encode rational numbers by a limited precision, they are not suitable for the packing operation.

4. EXPERIMENTAL RESULTS

We have implemented our algorithm presented in section 3 and compared the performance with the original spread spectrum watermarking technique [4]. Since the basic algorithm of our scheme is Cox's scheme with a limited precision, we evaluate the degradation of image quality by PSNR, and the detected correlation values. If the results are similar, we regard that the performance is not degraded. In our simulation, a standard gray-scaled image "lenna" of 256×256 pixels is used, and parameters are shown in Table 1. Even if p_w and p_x are added, the values of w_i and x_i might be negative. In such a case, the values are simply rounded to 0.

The differences with respect to the scaling parameters s_w and s_x are shown in Fig.1. According to the increase of such parameters, the precision of watermark signal and DCT coefficients are also increase. When $s_w = 2^0$, half elements of watermark signal become 0 because of the truncation of fractional part, hence the image quality is increased.

For the evaluation of correlation values, we embed a watermark signal using the original Cox's scheme and our scheme using the above parameters. The comparison of correlation values for the watermarked image which is not distorted by attacks is shown in Fig.2, where that of original scheme is 31.90 depicted by dot lines. From the figure, the performance is asymptotically reaching the original value according to the increase of the scaling factors s_w and s_x.

One of the important characteristic in the spread spectrum watermarking technique is the orthogonality of each watermark signal because of the robustness against collusion

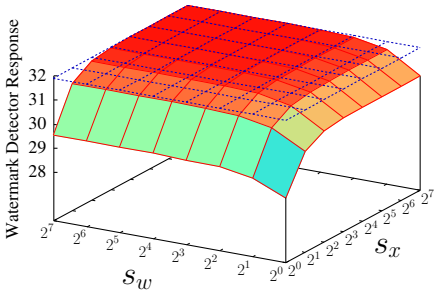

Figure 2: The correlation values.

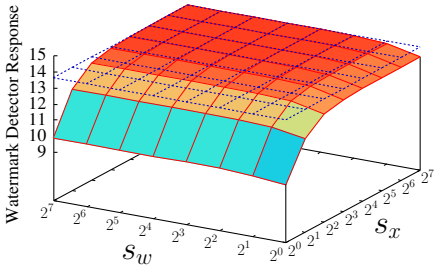

Figure 3: The comparison of average correlation value after averaging collusion attack for the scaling values s_w and w_x.

attack. It is well-known that the original scheme retains the robustness with a dozen of colluders. Under averaging collusion with 5 users, the average similarity value is 13.64. For the comparison, the average values in our scheme is shown in Fig.3, where dot lines means the average of original one. We also evaluate the robustness against the combination of collusion attack and JPEG compression because the compression of digital contents is a realistic assumption what attackers will do. By setting the quality parameter of JPEG compression 35%, the correlation values are computed, which comparison is shown in Fig.4, where the average value of original scheme is 10.10.

From the above results, the degradation of performance from the original scheme is very slight, and it does not affect the robustness against attacks. It is noted that the scaling factors s_w and s_x is closely related to the degradation of performance. It is better to increase the value of these parameters, for example $s_w \geq 2^3$ and $s_x \geq 2^3$, but we have to

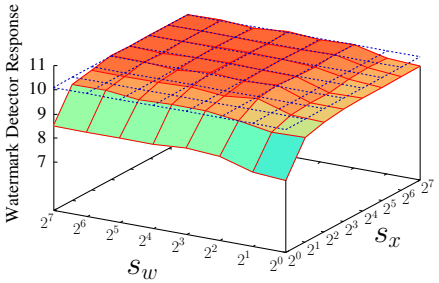

Figure 4: The comparison of the average correlation value after averaging collusion attack and JPEG compression for the scaling values s_w and w_x.

consider the communication costs because the bit-length to represent the watermarked DCT coefficient $\overline{x}_i + \alpha \overline{w}_i |\overline{x}_i|$ is increased according to the size of s_w and s_x, which degrades the coding rate of such information. For other images, "aerial", "baboon", "barbala", "f16", "girl", and "peppers", the similar results are derived with the above parameters. The attenuation of the correlation value from the original one is at most 0.3%, and under averaging collusion the attenuation is less than 1%. As the consequence, recommended parameters are $s_w = 2^3$ and $s_x = 2^3$ from our simulation results. It is expected that other kinds of spread spectrum watermarking schemes will be simulated with the similar precision, and the implementation is our future work.

When we use the above recommended parameters, the value of $\overline{x}'_i$ can be represented by 20 bits (the range must be within [0,1048576] if $s_w = s_x = 2^3$ and $p_x = 5000$). For the security reason, the bit-length of a composite $n = pq$ for the modulus of Paillier cryptosystem should be no less than 1024 bits. When $|n| = 1024$, an 1024-bit message is encrypted to an 2048-bit ciphertext. Under the above condition, the number of watermarked DCT coefficients in one ciphertext is at most 51 $(= \lfloor 1024/20 \rfloor)$. Since the number of DCT coefficients are $65536 = 256 \times 256$, the number of ciphertexts is 1285 $(= \lfloor 65536/51 \rfloor)$ and the total size of the ciphertexts is about 330KB, which is about 5 times larger than the original file size 66KB. In case the packing is not performed, the total size is more than 67MB. Therefore, the proposed method efficiently implement the Cox's spread spectrum watermarking scheme in the asymmetric fingerprinting protocol.

5. CONCLUSION

In this paper, we discuss about the implementation of the fingerprinting protocol based on the additive homomorphic property of public-key cryptosystems. The effects of rounding operation which maps a real value into a positive integer are formulated, and an auxiliary operation to obtain a watermarked content is presented. From our simulation results, the identification capability of our algorithm is quite similar to the Cox's algorithm, hence we can simulate the scheme on the cryptographic protocol with a limited precision.

Acknowledgment

This research was partially supported by the Ministry of Education, Culture, Sports Science and Technology, Grant-in-Aid for Young Scientists (B).

REFERENCES

[1] S. Katzenbeisser and F. A. P. Petitcolas, *Information hiding techniques for steganography and digital watermarking*, Artech house publishers, 2000.

[2] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inform. Theory*, vol. 44, no. 5, pp. 1897–1905, 1998.

[3] 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, 2003.

[4] I. Cox, J. Kilian, F. Leighton, and T. Shamson, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 5, pp. 1673–1687, 1997.

[5] B. Pfitzmann and A. Sadeghi, "Coin-based anonymous fingerprinting," in *Advances in Cryptology – EUROCRYPT'99*. 1999, vol. 1592 of *LNCS*, pp. 150–164, Springer-Verlag.

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

[7] M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2129–2139, 2005.

[8] C. Lei, P. Yu, P. Tsai, and M. Chan, "An efficient and anonymous buyer-seller watermarking protocol," *IEEE Trans. Image Process.*, vol. 13, no. 12, pp. 1618–1626, 2004.

[9] T. Okamoto and S. Uchiyama, "A new public-key cryptosystem as secure as factoring," in *Advances in Cryptology – EUROCRYPT'98*. 1998, vol. 1403 of *LNCS*, pp. 308–318, Springer-Verlag.

[10] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology – EUROCRYPT'99*. 1999, vol. 1592 of *LNCS*, pp. 223–238, Springer-Verlag.

[11] B. Chen and G.W.Wornel, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," *IEEE Trans. Inform. Theory*, vol. 47, no. 4, pp. 1423–1443, 2001.

[12] J. P. Prins, Z. Erkin, and R. L. Lagendijk, "Anonymous fingerprinting with robust qim watermarking techniques," *EURASIP J. Inform Security*, vol. 2007, no. 8, 2007.

[13] H. Zhao, M. Wu, Z. Wang, and K. J. R. Liu, "Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting," *IEEE Trans. Image Process.*, vol. 14, no. 5, pp. 646–661, 2005.

[14] Z. J. Wang, M. Wu, H. Zhao, W. Trappe, and K. J. R. Liu, "Anti-collusion forensics of multimedia fingerprinting using orthogonal modulatio," *IEEE Trans. Image Process.*, vol. 14, no. 6, pp. 804–821, 2005.

[15] Y. Zhu, D. Feng, and W. Zou, "Collusion secure convolutional spread spectrum fingerprinting," in *Proc. IWDW2005*. 2005, vol. 3710 of *LNCS*, pp. 67–83, Springer-Verlag.

[16] Y. Yacobi, "Improved boneh-shaw content fingerprinting," in *Proc. CT-RSA*. 2001, vol. 2020 of *LNCS*, pp. 378–391, Springer-Verlag.

[17] I. Damgård and Mats Jurik, "A generalisation, a simplification and some applications of paillier's probabilistic public-key system," in *Proc. of PKC '01*. 2001, vol. 1992 of *LNCS*, pp. 119–136, Springer-Verlag.

[18] P. A. Fouque, J. Stern, and G. J. Wackers, "Cryptocomputing with rationals," in *Proc. of Finalcial Cryptography*. 2003, vol. 2357 of *LNCS*, pp. 136–146, Springer-Verlag.

[19] C. Orlandi, A. Piva, and M. Barni, "Oblivious neural network computing via homomorphic encryption," *EURASIP J. Inform. Security*, vol. 2007, no. 9, 2007.