CDMA 技術に基づく電子指紋方式の電子指紋プロトコルへの実装

栗林 稔　　森井 昌克

神戸大学大学院工学研究科
657-8501 兵庫県神戸市灘区六甲台町 1-1

{kminoru, mmorii}@kobe-u.ac.jp

あらまし　マルチメディアコンテンツのための電子指紋技術は，指紋情報の生成，埋め込み処理，不正コピーからの追跡などを含んでいる．購入者の権利を守るためには，売買プロセスにおいて非対称性が求められており，暗号プロトコルにより実現する方法が提案されている．我々は，Coxらの電子透かし手法をこの暗号プロトコルに適用する手法を提案してきた．本稿では，我々の研究グループで提案したCDMA 技術に基づく電子指紋手法を，準同型暗号を用いた電子指紋プロトコルに適用する手法を提案する．まず，実数を整数に変化させる丸め処理とその影響について調べ，ロバスト性と通信オーバヘッド間のトレードオフについて従来手法と評価する．

Implementation of CDMA-Based Fingerprinting Scheme in Asymmetric Fingerprinting Protocol

Minoru Kuribayashi　　Masakatu Morii

Graduate School of Engineering, Kobe University
1-1, Rokkodai-Cho, Nada-Ku, Kobe-Shi, Hyogo 657-8501 Japan

{kminoru, mmorii}@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 copy. Considering a buyer's right, the asymmetric property in the transaction between a buyer and a seller must be achieved using a cryptographic protocol. We have proposed the implementation method of Cox's watermarking scheme in the protocol. In this paper, we propose the method for implementing the CDMA-based fingerprinting scheme in the fingerprinting protocol based on the homomorphic encryption scheme. We first develop a rounding operation which converts a real value into an integer and its compensation, and then explore the trade-off between the robustness and communication overhead.

1 Introduction

Fingerprinting technique can dissuade people from executing illegal redistribution of digital contents by making it possible to identify the original buyer of the redistributed copy. The technique can be classified into two categories; one is the generation of fingerprint information, and the other is the secure protocol between a buyer and seller. Since each user purchases the copy involving his own fingerprint, the fingerprinted copy slightly differs with each other. Therefore, a coalition of users will combine their different marked copies of a same content for the purpose of removing/changing the original fingerprint. It is important to generate fingerprints that can tolerate the collusion attack. After the transaction protocol between the buyer and seller, if both of the parties get a fingerprinted copy, the seller may frame the buyer by distributing the copy by himself. On the contrary, the buyer can distribute a pirated copy but later repudiate it by insisting that it came from the seller. For the solution of such a threat of dispute, the asymmetric property that only a seller can get the fingerprinted copy was introduced in the fingerprinting protocol [1].

Pfitzmann et al. [2] introduced the digital cash scheme to a fingerprinting protocol. In the scheme, bit commitment schemes are exploited for the embedding of fingerprint using zero-knowledge proof. Lei et al. [3] introduced a trusted authority who generates a robust fingerprint to reduce the communication costs. In [4], the enciphering rate is drastically improved using a public-key cryptosystem with an additive homomorphism. Although the homomorphic property is effective for constructing asymmetric fingerprinting, there are still problems in its implementation. In [9], the Cox's watermarking method [8] is implemented in the asymmetric fingerprinting protocol introducing a rounding and post-processing operations. Though it can simulate the original Cox's method, it sacrifices the enciphering rate to maintain the traceability.

In this paper, we propose the method for implementing the CDMA-based fingerprinting scheme. For the implementation, the fingerprint sequence and frequency components of an image that are represented by real values must be rounded to apply the public-key cryptosystem. For the characteristic of the fingerprinting protocol, frequency components and the fingerprint sequence must be separately encrypted after quantization. Due to the simple embedding procedure, the overhead required for the implementation is much smaller than the conventional study [9].

2 Preliminaries

2.1 Fingerprinting Protocol

In order to achieve an asymmetric property, the homomorphic property of public-key cryptosystems is introduced in the fingerprinting protocols.

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

$$g(E(M_1), E(M_2)) = E(f(M_1, M_2)), \qquad (1)$$

where $g(\cdot)$ and $f(\cdot)$ is one of the operations, *addition, multiplication, XOR,* etc. If M_1 is regarded as a digital content and M_2 as a fingerprint, the fingerprint can be embedded in the content without decryption by multiplying those ciphertexts. Since they are calculated using a buyer's public encryption-key, the fingerprinted copy is decrypted only by the buyer, hence the asymmetric property is satisfied. The embedding operation based on the homomorphic property is basically performed for each element of fingerprint information which will be composed of bit-sequence or spread spectrum sequence.

The fingerprinting protocol in [3] introduced a trusted authority who generates a robust fingerprint when valid items of a certain transaction between a buyer and a seller are transmitted from a seller. Different from the zero-knowledge protocol applied in [2], the issue of fingerprint information is committed to the authority to reduce the additional communication costs. In [3], 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), where pk and sk are the public and secret keys of public-key cryptosystem, respectively. He sends pk, which is a pseudonym associated with B, to CA in order to get an anonymous certificate $Cert_{\texttt{CA}}(pk)$. When B makes an order to a seller S, he checks the validity of $Cert_{\texttt{CA}}(pk)$. Then S asks WCA to generate a unique watermark $\boldsymbol{w}$ for the current transaction between B and S. The detail is referred to [3].

2.2 Implementation of Watermarking Method

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 [4], the quantization index modulation based watermarking technique (QIM) [5] is applied for the embedding procedure because it rounds the values of frequency components in integers. Prins et al. [6] 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. In order to exploit the message space effectively, dozens of fingerprinted frequency components are packed in one message in [4], 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 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 [5] and its variants [6]. In [7], the adaption of Cox's spread spectrum watermarking scheme [8] is discussed. In [9], considering the effects of rounding operation which maps a real value into a positive integer, an auxiliary operation to obtain a fingerprinted copy is presented. Due to the multiplicative watermarking procedure of the Cox's method, the auxiliary operation increases the communication costs. Furthermore, the computational complexity of the Cox's method is linearly increased with respect to the number of users.

2.3 CDMA-Based Fingerprinting

In [10], we have proposed a collusion-resilient fingerprinting scheme based on the CDMA technique, which is a kind of additive watermarking method.

We suppose that each user's fingerprint consists of two parts of information; "group ID" is to identify the group where a user belongs to and "user ID" represents an individual user in the group. For such fingerprint information (i_g, i_u), two spread spectrum sequences are given by

$$\boldsymbol{w_{i_g}} = \boldsymbol{pn(s)} \otimes \boldsymbol{dct(i_g, \beta_g)}, \qquad (2)$$

$$\boldsymbol{w_{i_u}} = \boldsymbol{pn(i_g)} \otimes \boldsymbol{dct(i_u, \beta_u)}, \qquad (3)$$

respectively, where $\boldsymbol{pn(s)}$ is a PN sequence 1 and -1 values generated using an initial value s, $\boldsymbol{dct(i, \beta)}$ is i-th DCT basic vector of ℓ-tuple with a strength β, and $\otimes$ means elementwise multiplication. The fingerprint sequence $\boldsymbol{w_{i_g}} + \boldsymbol{w_{i_u}}$ is embedded into the frequency components of an image.

Notice that $\boldsymbol{w_{i_u}}$ is binded with group ID i_g. It allows us to make a hierarchical structure, which increases the number of users; ℓ^2 users with only 2ℓ spectrum components. Then, we can identify colluders from the combination of detected group ID and user ID. Such a hierarchical structure also contributes on the reduction of the computational costs required at the detection.

The procedure to embed a user's fingerprint into $N \times N$ image is summarized as follows.

1. Perform full-domain DCT to an image.
2. Select ℓ DCT coefficients from low and middle frequency domain based on a secret key key. We denote the selected coefficients by $\boldsymbol{v} = \{v_0, \ldots, v_{\ell-1}\}$.
3. Generate two spectrum sequences $\boldsymbol{w_{i_g}}$ and $\boldsymbol{w_{i_u}}$ given in Eqs.(2) and (3) using a secret key s, (i_g, i_u), β_g, and β_u.
4. Embed the spectrum sequences into $\boldsymbol{v}$ by addition.
$$\boldsymbol{v}^\star = \boldsymbol{v} + \boldsymbol{w_{i_g}} + \boldsymbol{w_{i_u}} \qquad (4)$$
5. Perform full-domain IDCT to obtain a fingerprinted image.

Using a fast DCT algorithm, the computational complexity at the detection can be reduced (See [10]). The traceability was further improved by the iterative detection with the removal operation such that detected signals, which are regarded as the interference for the remained signals, are sequentially removed from a detection sequence [11].

3 Proposed Method

Now, we implement the CDMA-based fingerprinting scheme [10] on the fingerprinting protocol proposed by Lei et al. [3]. We assume that an original image is composed of $M \times N$ pixels and is represented by the DCT selected coefficients $v_j, (1 \leq j \leq \ell)$ and the remaining ones $v_j, (\ell + 1 \leq j \leq MN)$. For simplicity, a fingerprint sequence is denoted by $\boldsymbol{w} = \{w_1, w_2, \ldots, w_\ell\}$.

3.1 Embedding

The embedding operation in Eq.(4) can be easily performed using the additive homomorphic property of public-key cryptosystems. It is represented by the multiplication as follows.

$$E_{pk}(v_j + w_j) = E_{pk}(v_j) \cdot E_{pk}(w_j) \qquad (5)$$

Here, it is noticed that a fingerprint signal and DCT coefficients are generally represented by real values and they must be rounded to integers 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 numbers should be avoided considering the property of a cryptosystem. In our method, constant positive integers p_w and p_v are added to the fingerprint signals w_j and DCT coefficients v_j, respectively.

At first, we show the operation concerning to a fingerprint signal. Since the ciphertext of $\boldsymbol{w}$ is computed by a watermark certification authority `WCA`, the enciphering operation is performed previously sent to a seller `S`. A constant positive integer p_w is added to each element of fingerprint signal $w_j, (1 \leq j \leq \ell)$ to make the value positive. Then, it is scaled by a factor of s in order to keep the degree of precision, and it is quantized to $\overline{w}_j$. Such operations are formalized by the following one equation;

$$\begin{aligned} \overline{w}_j &= int(s(w_j + p_w)), \\ &= s(w_j + p_w) + \epsilon_{w_j} \ 1 \leq i \leq \ell, \end{aligned} \qquad (6)$$

where $int(a)$ outputs the nearest integer from a real value a, and ϵ_{w_j} is the quantization error of $\overline{w}_j$. After the operation, `WCA` encrypts $\overline{\boldsymbol{w}} = \{\overline{w}_1, \overline{w}_2, \ldots, \overline{w}_\ell\}$ using a public key pk, and the ciphertexts

$$E_{pk}(\overline{\boldsymbol{w}}) = \{E_{pk}(\overline{w}_1), E_{pk}(\overline{w}_2), \ldots, E_{pk}(\overline{w}_\ell)\}, \qquad (7)$$

p_w and s are sent to `S`.

Next, `S` performs the rounding operation to DCT coefficients $v_j, (1 \leq j \leq \ell)$ as follows. A positive integer value p_v is added to each DCT coefficient, and then scaled by s. By quantizing it, the rounded DCT coefficient $\overline{v}_j$ is obtained.

$$\begin{aligned} \overline{v}_j &= int(s(v_j + p_v)), \\ &= s(v_j + p_v) + \epsilon_{v_j}, \ 1 \leq j \leq \ell, \end{aligned} \qquad (8)$$

where ϵ_{v_j} is the quantization error of $\overline{v}_j$. `S` embeds $\overline{w}_j$ into $\overline{v}_j$ for $1 \leq j \leq \ell$ based on the additive homomorphic property of public cryptosystem as follows.

$$E_{pk}(\overline{v}_j) \cdot E_{pk}(\overline{w}_j) = E_{pk}(\overline{v}_j + \overline{w}_j) \qquad (9)$$

Then, the plain value of the ciphertext $E_{pk}(\overline{v}_j + \overline{w}_j)$ is

$$\begin{aligned} \overline{v}_j + \overline{w}_j &= s(v_j + w_j) + s(p_v + p_w) \\ &\quad +(\epsilon_{v_j} + \epsilon_{w_j}). \end{aligned} \qquad (10)$$

It is noticed that the remaining DCT coefficients $v_j, (\ell + 1 \leq j \leq MN)$ should be sent to `B`. In order to keep the secrecy of the embedding position, they must be encrypted before delivery. Without the loss of generality, the rounding operation for those coefficients are given by

$$\begin{aligned} \overline{v}_j &= int(s(v_j + s(p_v + p_w)), \\ &= s(v_j + p_v + p_w) + \epsilon_{v_j}, \end{aligned} \qquad (11)$$

and the ciphertexts $E_{pk}(\overline{v}_j)$ are sent with the fingerprinted ones $E_{pk}(\overline{v}_j + \overline{w}_j)$, s, and $p = p_w + p_v$ to `B`.

3.2 Decryption and Post-Processing

After the decryption of the received ciphertexts, `B` divides the results by the scaling factor s, and then subtracts an adjustment factor p as the post-processing operation .

At the embedding position, the ciphertexts are $E_{pk}(\overline{v}_j + \overline{w}_j)$ and the post-processing operation outputs the fingerprinted DCT coefficients $v_j^\star, 1 \leq j \leq \ell$ as follows;

$$\begin{aligned} v_j^\star &= \frac{D_{sk}(E_{pk}(\overline{v}_j + \overline{w}_j))}{s} - p \qquad (12) \\ &= (v_j + w_j) + \epsilon_j \qquad (13) \end{aligned}$$

where $D_{sk}(\cdot)$ is a deciphering function using a secret key sk and ϵ_j is the total rounding error represented by

$$\epsilon_j = \frac{\epsilon_{v_j} + \epsilon_{w_j}}{s}. \tag{14}$$

At the other position, the ciphertexts are $E_{pk}(\overline{v}_j)$ and $\mathtt{B}$ obtains $v_j^\star, \ell + 1 \le j \le MN$ after the post-processing operation.

$$\begin{aligned} v_j^\star &= \frac{D_{sk}(E_{pk}(\overline{v}_j))}{s} - p & (15) \\ &= v_j + \frac{\epsilon_{v_j}}{s}. & (16) \end{aligned}$$

It is remarkable that the embedding position is kept secret from $\mathtt{B}$, the classification of the above operations is difficult.

In the CDMA-based fingerprinting method, a fingerprint sequence is composed of two orthogonal sequences $\boldsymbol{w_{i_g}}$ and $\boldsymbol{w_{i_u}}$ with energy β_g^2 and β_u^2, respectively. Under the assumption that the fingerprint sequence of length ℓ follows Gaussian distribution with zero mean, the variance is calculated as $\sigma_w^2 = (\beta_g^2 + \beta_u^2)/\ell$. From the statistical property, when a parameter p_w is given, the error probability that $w_j + p_w$ is less than 0 is given by

$$\Pr(w_j + p_w < 0) = \frac{1}{2}\mathrm{erfc}\left(\frac{p_w}{\sqrt{2\sigma_w^2}}\right), \tag{17}$$

where erfc() stands for the complementary error function. When $w_i + p_w$ is less than 0, such a value is rounded to 0 in order to avoid the underflow.

4 Experimental Results

The degradation of fingerprints are evaluated by the number of detected colluders. If the results are close to the original ones, we regard that the performance of our implemented method is not degraded. In our simulation, a standard gray-scaled image "lena" of 512×512 pixels is used. The energy of embedding signals is fixed in our simulation by $\beta_g = 400$ and $\beta_u = 600$, respectively. The detection of the fingerprint is performed with the knowledge of the host image. For the evaluation under an equal condition, the number of users is fixed to 2^{20} for different lengths $\ell = 1024$, 2048, 4096.

Table 1: The error probability $\Pr(w_j + p_w < 0)$ when $p_w = 64$.

ℓ	σ_w^2	$\Pr(w_j + p_w < 0)$
1024	507.81	4.51×1^{-3}
2048	253.91	5.91×1^{-5}
4096	126.95	1.25×1^{-8}

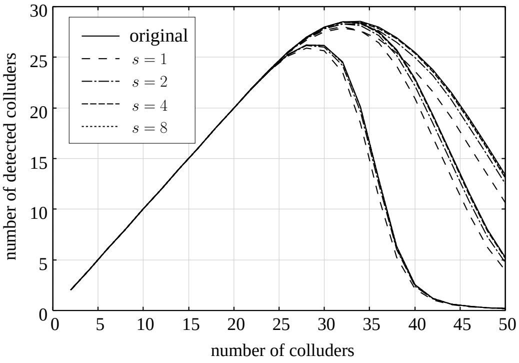

Figure 1: Comparison of the number of detected colluders.

We set constant values $p_w = 64$ and $p_v = 5000$ to make w_j and v_j positive. Even if p_w and p_v are added, some of them might be negative. In such a case, the values are simply rounded to 0. When $p_w = 64$, the error probability $\Pr(w_j + p_w < 0)$ is calculated as shown in Table 1. The table indicates that, in average, $4.5 (= \Pr(w_j + p_w < 0) \times \ell)$ elements might be negative if $\ell = 1024$. In the following simulation, the number of simulation is 10^4 times, and the results are the averaged values.

The comparison of the detected number of colluders is shown in Fig.1. We can see that the performance is asymptotically reaching the original curve according to the increase of the scaling factor s, and the curve becomes very close to the original one if $s \ge 4$.

The error (false-positive) probability is an important factor to evaluate the performance of fingerprinting scheme. Table 2 shows the number of false-positive detection N_{FP}. From the results, we can say that the error probability of our method is very similar to that of original one.

When we use the parameters $s = 4$, $p_w = 64$, and $p_v = 5000$, the value of $\overline{v}_i^\star$ can be repre-

Table 2: Comparison of the number of false-positive N_{FP}.

	$N_{FP}(\times 10^{-4})$				
ℓ	org	$s=1$	$s=2$	$s=4$	$s=8$
1024	2.60	2.24	2.64	3.20	2.96
2048	0.92	1.28	1.12	1.60	0.96
4096	0.96	1.44	0.68	1.20	1.20

sented by 16 bits (the range must be within $[0,\ 2^{16}-1]$). As the original pixel value is represented by 8 bits, the required memory for our implementation is 2-times bigger, while the implementation of Cox's method given in [9] requires 20 bits for each elements. Therefore, the exploitation of CDMA-based fingerprinting is suitable in this regards.

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 fingerprinted copy is presented. From our simulation results, the identification capability of our algorithm is quite similar to the original CDMA-based fingerprinting scheme.

Acknowledgment

This research was partially supported by the Ministry of Education, Culture, Sports Science and Technology, Grant-in-Aid for Young Scientists (B) (21760291), 2009.

References

[1] B. Pfitzmann and M. Schunter, "Asymmetric fingerprinting," Advances in Cryptology – EUROCRYPT'96, LNCS, vol.1070, pp.84–95, Springer-Verlag, 1996.

[2] B. Pfitzmann and A. Sadeghi, "Anonymous fingerprinting with direct non-repudiation," Advances in Cryptology – ASIACRYPT'2000, LNCS, vol.1976, pp.401–414, Springer-Verlag, 2000.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

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

[8] I.J. Cox, J. Kilian, F. Leighton, and T. Shamson, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol.6, no.12, pp.1673–1687, 1997.

[9] M. Kuribayashi and M. Morii, "On the implementation of asymmetric fingerprinting protocol," Proc. of EUSIPCO2008, pp.SS7–1, 2008.

[10] N. Hayashi, M. Kuribayashi, and M. Morii, "Collusion-resistant fingerprinting scheme based on the CDMA-technique," Proc. of IWSEC2007, LNCS, vol.4752, pp.28–43, Springer-Verlag, 2007.

[11] M. Kuribayashi and M. Morii, "Iterative detection method for cdma-based fingerprinting scheme," IH 2008, LNCS, vol.5284, pp.357–371, Springer, Heidelberg, 2008.