Iterative Detection Method for CDMA-based Fingerprinting Scheme

Minoru Kuribayashi[1] and Masakatu Morii[1]

Graduate School of Engineering, Kobe University
1-1 Rokkodai-cho, Nada-ku, Kobe, 657-8501 Japan.
{kminoru,mmorii}@kobe-u.ac.jp

Abstract. Digital fingerprinting of multimedia data involves embedding information in the content signal and offers the traceability of illegal users who distribute unauthorized copies. One potential threat to fingerprinting system is collusion, whereby a group of users combines their individual copies in an attempt to remove the underlying fingerprints. Hayashi et. al have proposed hierarchical fingerprinting scheme using the CDMA technique which designed a fingerprint signal by a combination of quasi-orthogonal sequences to increase the allowable number of users. In this paper, we formalize the model of collusion from the viewpoint of a communication channel, and propose a removal operation considering the interference among fingerprints. We also explore the characteristic of the proposed detector and the effects of the removal operation on a detection sequence. By introducing two kinds of thresholds for the determination of the presence of fingerprints, the performance of the proposed detector is enhanced effectively.

1 Introduction

Digital fingerprinting is used to trace the illegal users, where a unique ID known as digital fingerprints [1] is embedded into a content before distribution. When a suspicious copy is found, the owner can identify illegal users by extracting the fingerprint. The research on fingerprinting techniques is classified into two studies; The designs of collusion-resistant fingerprint and secure cryptographic protocol. Since each user purchases a content involving his own fingerprint, each content is slightly different. A coalition of users will therefore combine their different marked copies of a same content for the purpose of removing/changing the original fingerprint. The other threats in the fingerprinting are dispute and repudiation of a purchase. The purpose of cryptographic protocols is to solve such threats by achieving the asymmetric property [2]. In spite of the property, the production of embedding information is based on the design of collusion resistant fingerprint.

One of the simple approaches for the collusion attack is to average multiple copies of a same content. By combining many copies sufficiently, the fingerprints will be weakened or removed by the attack. It is important to generate fingerprints that can be not only to identify the colluders, but also resilient against

the collusion attack. 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 [3–6], and the other approach is to devise an exclusive code, known as collusion-secure code [7–10], which has traceability of colluders.

The origin of the spread spectrum fingerprinting is Cox's method that embeds the sequence into the frequency components of a digital image and detects it using a correlator [3]. Since normally distributed values allow the theoretical and statistical analysis of the method, modeling of a variety of attacks have been studied. Studies in [4] 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 fingerprinting scheme are based on the Cox's method, especially for the usage of the sequence which elements are randomly selected from normally distributed values. Instead of such a random sequence, theoretically quasi-orthogonal sequences are designed in [11] using a PN sequence such as M-sequence and Gold-sequence [12], etc. combined with orthogonal transform like DCT, which basic idea is the exploitation of the CDMA technique. Using the orthogonality, it is possible to assign a unique combination of spectrum components to each user and provide a hierarchical structure using two kinds of SS sequences; one is for group ID, and the other for user ID. At a detection of the fingerprint information, we list the components which signal strengths exceed a threshold, and identify the corresponding colluders whose fingerprints are expressed by the combination of the listed components. After the detection of group ID, we detect each user ID which is corresponding to each group ID since the group ID is required for generating the detection sequence to examine the user ID within the group. Therefore, if we fail to detect the group ID at the first detection, the following procedure to detect user ID does not conducted, hence the probability of correct detection of user's fingerprint falls. In order to solve this problem, the threshold for a group ID is designed lower. Even if wrong group IDs are accidentally detected, user IDs associated with the wrong group IDs will be excluded with high probability.

Although the interference among inserted signals under averaging collusion is expected very small, the effects become considerably high with an increase of number of colluders. Here, it is remarkable that detected signals are assumed as the interference of other undetected signals. In this paper, we formalize the model of the CDMA-based fingerprinting scheme, and present a removal operation to minimize the interference. In [13], the analysis of collusion attacks for uniformly distributed watermarks employing one to two dozen independent copies of watermarked content. We further analyze the effects on the watermarks caused by the collusion attacks using the formalized model of the CDMA-based fingerprinting scheme, and it helps us to remove the noise signals involved in detection sequences from a pirated copy. Because the sequences contain some colluders' fingerprint signals, they work as an interference at the detection of each objective signal. Once a fingerprint signal is detected, the signal is removed from the detection sequence for the decrease of interference in our method. The

effects of the removal operation on the detection sequence are explored, and the operation is adaptively customized. It is obvious that lower threshold for a group ID not only improves the true-positive detection rate, but also degrades the false-positive rate. Then, if wrong group IDs are accidentally detected, the signals which contain the undetected fingerprints' signals are removed regarding as the interference. In order to avoid such a removal as much as possible, two kinds of thresholds are introduced; one is for the detection of candidates for group ID, and the other is for the determination of removal operation. If detected signals for group IDs retain sufficiently large energy, clearly they are determined as the embedded fingerprints, otherwise they are listed as potential suspects. By separating the detected signals into such two cases using two thresholds, the removal operation is selectively performed in the proposed scheme. Final decision for the identification of colluders is based on a higher threshold for a user ID. Due to the successive removal of such signals, we can extract more objective signals of colluders and less that of innocent users.

2 CDMA-Based Fingerprinting

Hayashi et. al have proposed a CDMA-based fingerprinting scheme with high robustness against collusion attack [11]. In this section, we review the basic idea, and summarize the embedding/detection procedure with an hierarchical structure.

2.1 Basic Idea

Let a sequence $\boldsymbol{d} = \{d_0, \ldots, d_{\ell-1}\}$ be constructed from DCT coefficients and be initialized to the zero vector. We assume that the i-th element d_i is assigned to the i-th user as a fingerprint and embedding strength β is added to it; Only i-th DCT coefficient retains strength β. Then, a spread spectrum sequence assigned to the i-th user is given by

$$\boldsymbol{w_i} = \boldsymbol{pn(s)} \otimes \boldsymbol{dct(i, \beta)}, \tag{1}$$

where $\boldsymbol{pn(s)}$ is a PN sequence generated using an initial value s, $\boldsymbol{dct(i, \beta)}$ is the i-th DCT basic vector of an ℓ-tuple of strength β, and $\otimes$ implies element-wise multiplication. The sequence $\boldsymbol{w_i}$ is embedded into the frequency components of a digital image.

At the detection, a sequence $\tilde{\boldsymbol{w}}_{\boldsymbol{i}}$ is extracted from the difference between an original image and a pirated one. Then, instead of the similarity measurement [3], we multiply a PN sequence and perform DCT to obtain the sequence $\tilde{\boldsymbol{d}} = \{\tilde{d}_0, \ldots, \tilde{d}_{\ell-1}\}$;

$$\tilde{\boldsymbol{d}} = \mathsf{FDCT}(\boldsymbol{pn(s)} \otimes \tilde{\boldsymbol{w}}_{\boldsymbol{i}}), \tag{2}$$

where FDCT means fast discrete cosine transform algorithm. Illegal users can be determined if the corresponding coefficients exceed a threshold T.

The advantage of the detection method in a CDMA-based fingerprinting scheme [11] is the computational complexity because of the fast algorithm of DCT which requires $\mathrm{O}(\ell \log \ell)$ operations [14].

2.2 Hierarchical Embedding Procedure

We suppose that each user's fingerprint information consists of two parts; "group ID," identifies the group to which a user belongs; and "user ID," represents an individual user within the group.

Exploiting the quasi-orthogonal property of a PN sequence, we introduce a dependency between the spread spectrum sequences generated from two sequences $\boldsymbol{d_g}$ and $\boldsymbol{d_u}$. Before embedding a user ID, its corresponding DCT basic vector with strength β_g is multiplied by a specific PN sequence related to $\boldsymbol{d_g}$. Thus, for fingerprint information (i_g, i_u), two spread spectrum sequences related to $\boldsymbol{d_g}$ and $\boldsymbol{d_u}$ with strength β_g and β_u are given by

$$\boldsymbol{w_{i_g}} = \boldsymbol{pn(s)} \otimes \boldsymbol{dct(i_g, \beta_g)}, \tag{3}$$

$$\boldsymbol{w_{i_u}} = \boldsymbol{pn(i_g)} \otimes \boldsymbol{dct(i_u, \beta_u)}, \tag{4}$$

respectively. Notice that $\boldsymbol{w_{i_u}}$ is bounded to the group ID i_g. The spectrum sequences are mutually independent if the applied PN sequences are different. Thus, an hierarchical structure is realized, which increases the number of users; ℓ^2 users with only 2ℓ spectrum components.

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

1. Perform full-domain DCT on the image.
2. Select ℓ DCT coefficients from low- and middle-frequency domains on the basis of 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 $\boldsymbol{w_{i_u}}$ by using a secret key s, (i_g, i_u), β_g, and β_u.
4. Embed the spectrum sequences into $\boldsymbol{v}$ by addition.

$$\boldsymbol{v}^* = \boldsymbol{v} + \boldsymbol{w_{i_g}} + \boldsymbol{w_{i_u}} \tag{5}$$

5. Perform full-domain IDCT to obtain a fingerprinted image.

From the viewpoint of the CDMA technique, it is possible to detect $\boldsymbol{w_{i_g}}$ and $\boldsymbol{w_{i_u}}$ from $\boldsymbol{v}^*$ because of the quasi-orthogonal property.

2.3 Detection

At a detector side, an host image (host frequency components) and secret keys *key* and s are required. Since the group ID ig and the user ID i_u that comprise a user's fingerprint are embedded separately, the detection procedure consists of two stages. The first stage focuses on identifying groups involving colluders, and the second one is to identify colluders within each guilty group. The latter operation is performed on the sequence using the PN sequence generated from the identified group ID as a seed. At the detection of each ID, we compare the components in the detection sequence with a threshold.

The detection sequence is obtained by performing DCT after subtracting the host sequence from that of a pirated copy, which is denoted by $\tilde{\boldsymbol{d}} = \{\tilde{d}_0, \ldots, \tilde{d}_{\ell-1}\}$. To apply statistical decision theory, we assume that $\tilde{\boldsymbol{d}}$ is composed of random variables and the sequence except for the fingerprinted component $\tilde{d}_k$, which is denoted by $\tilde{\boldsymbol{d}}$, are distributed according to $N(0, \sigma^2)$, where σ is the variance of the sequence. If we insert a watermark to add β to d_k in order to satisfy the inequality

$$\tilde{d}_k > \max_{i \neq k} \{\tilde{d}_i\}, \tag{6}$$

then we can detect the embedded watermark by setting a threshold T to be imposed $\tilde{d}_k > T > \tilde{d}_i$. If $\tilde{d}_i > T$, then a detector decides that d_i is watermarked, and hence, it detects an innocent user by mistake. Therefore, $\Pr(\tilde{d}_i > T)$ is the probability of false-positive detection. Then, we can say that

$$\Pr(\tilde{d}_i > T) \leq \frac{1}{2} \operatorname{erfc}\left(\frac{T}{\sqrt{2\sigma^2}}\right), \tag{7}$$

from study in [15]. The knowledge of the variance σ^2 enables a fingerprint detector to obtain a proper threshold corresponding to a given probability of false-positive detection.

Under the above characteristic of the detection sequence, illegal users are detected as follows.

1. Perform full-domain DCT on the pirated copy.
2. Select ℓ DCT coefficients from low- and middle-frequency domains on the basis of a secret key key, which is denoted by $\tilde{\boldsymbol{v}}$.
3. Detect a group ID by the following operations.
   3-1. Generate a PN sequence $\boldsymbol{pn(s)}$ using a secret key s, and multiply $\tilde{\boldsymbol{v}} - \boldsymbol{v}$ by it.
   3-2. Perform one-dimensional(1D) DCT to obtain the detection sequence $\tilde{\boldsymbol{d}}_{\boldsymbol{g}}$;

$$\tilde{\boldsymbol{d}}_{\boldsymbol{g}} = \mathsf{FDCT}\big(\boldsymbol{pn(s)} \otimes (\tilde{\boldsymbol{v}} - \boldsymbol{v})\big) \tag{8}$$

   3-3. Calculate the variance of $\tilde{\boldsymbol{d}}_{\boldsymbol{g}}$ by considering the property of its distribution (See [11]) and determine a threshold T_g with a given false-positive probability Pe_g.
   3-4. If $\tilde{d}_{g,k} \geq T_g, (0 \leq k \leq \ell - 1)$, determine k as the group ID i_g.
4. Detect a user ID using the detected group ID by the following operations.
   4-1. Generate a PN sequence $\boldsymbol{pn(i_g)}$, and multiply $\tilde{\boldsymbol{v}} - \boldsymbol{v}$ by it.
   4-2. Perform 1D DCT to obtain the detection sequence $\tilde{\boldsymbol{d}}_{\boldsymbol{u}}$;

$$\tilde{\boldsymbol{d}}_{\boldsymbol{u}} = \mathsf{FDCT}\big(\boldsymbol{pn(i_g)} \otimes (\tilde{\boldsymbol{v}} - \boldsymbol{v})\big) \tag{9}$$

   4-3. Calculate the variance of $\tilde{\boldsymbol{d}}_{\boldsymbol{u}}$ and determine a threshold T_u with a given false-positive probability Pe_u.
   4-4. If $\tilde{d}_{u,h} \geq T_u, (0 \leq h \leq \ell - 1)$, determine h as the user ID i_u.

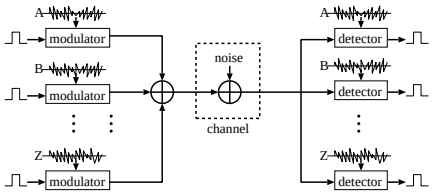

Fig. 1. The model of the CDMA technique.

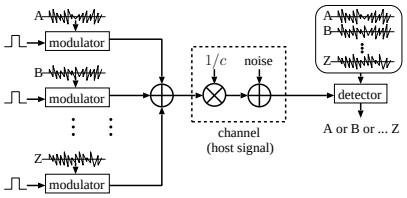

Fig. 2. The model of the CDMA-based fingerprinting scheme.

Note that when some group IDs are detected, we examine each user ID corresponding to each group ID in order to identify all colluders. Therefore, this fingerprinting scheme is designed for *catch many*-type fingerprinting [1].

The detection of colluders are performed selectively depending on the detected group IDs, and FDCT is performed only once for the detection of a group ID and a few dozens of times for the corresponding user IDs. Suppose that the number of detected group IDs is much smaller than ℓ and it strongly depends on the number of colluders c. Then, the required number of operation for our detection method is approximately given by $\mathrm{O}(c\ell \log \ell)$.

3 Proposed Detection Method

In this section, we formalize the averaging collusion as the CDMA channel and study the property of interference from noise elements. Based on the analysis, the interference can be removed efficiently from detection sequences in order to improve the true-positive detection rate.

3.1 Modeling

On the CDMA technique, signals of some users are multiplexed in one communication channel, and each detector checks the correlation with own PN sequence to decode an objective signal from the channel as shown in Fig.1. The CDMA-based fingerprinting scheme also follows the similar channel model except for the number of objective signals stored in a detector. Because the transmitting signals are assumed as the fingerprints of colluders and the objective signals should be correctly extracted from the channel which is an host signal. Since the host signal is known at the detector side, the received signal involves the objective signals and an additive noise. At the multiplexing process in a channel, the objective signals attenuate by a factor of the number of colluders, which is $1/c$, because of the effect of averaging. Such a channel model is illustrated in Fig.2. Our goal is to extract, not merely detect, the correct fingerprint signals as many as possible from the detection sequence with high probability.

The design of appropriate fingerprints must be complemented by the development of mechanisms that can capture those involved in the illegal user of

content. The detection of the signals, however, becomes difficult according to the increase of the number of colluders, and the difficulty is caused by the interference with each other. When a collusion occurs involving c colluders who form a pirated copy, the observed DCT coefficients after averaging collusion is

$$\tilde{\boldsymbol{v}} = \frac{1}{c}\sum_{t=1}^{c}\tilde{\boldsymbol{v}}_{\boldsymbol{t}} + \boldsymbol{\epsilon}, \tag{10}$$

where $\tilde{\boldsymbol{v}}_{\boldsymbol{t}}$ is the fingerprinted frequency components of the t-th colluder and $\boldsymbol{\epsilon}$ is an additive noise that follows a Gaussian distribution with zero mean. Note that the additive noise is caused by the rounding-off effects when IDCT is performed to obtain a fingerprinted image. In this model, the number of colluders and the additive noise are unknown parameters. Since the host signal is available in our scenario, the detected signal sequence is represented by

$$\tilde{\boldsymbol{v}} - \boldsymbol{v} = \frac{1}{c}\sum_{t=1}^{c}(\boldsymbol{w}_{\boldsymbol{i}_{\boldsymbol{g},t}} + \boldsymbol{w}_{\boldsymbol{i}_{\boldsymbol{u},t}}) + \boldsymbol{\epsilon}. \tag{11}$$

For the detection of a group ID, the PN sequence $\boldsymbol{pn(s)}$ is multiplied and DCT is performed as explained in Eq.(8). It is remarkable that the detection sequence $\tilde{\boldsymbol{d}}_{\boldsymbol{g}}$ involves the noise signal $\boldsymbol{pn(s)} \otimes (\sum_{t=1}^{c} \boldsymbol{w}_{\boldsymbol{i}_{\boldsymbol{u},t}}/c + \boldsymbol{\epsilon})$ as well as the signal corresponding to the colluders' group ID $\boldsymbol{pn(s)} \otimes (\sum_{t=1}^{c} \boldsymbol{w}_{\boldsymbol{i}_{\boldsymbol{g},t}}/c)$. Although such a noise signal retains quasi-orthogonality, the effects are not negligible when the number of colluders is increased. The same effects are occurred at the detection of a user ID.

From the viewpoint of energy, the embedded signal strength β_g and β_u is attenuated into β_g/c and β_u/c, respectively. Notice that since the sequences $\tilde{\boldsymbol{d}}_{\boldsymbol{g}}$ and $\tilde{\boldsymbol{d}}_{\boldsymbol{u}}$ are transformed from the sequence $\tilde{\boldsymbol{v}} - \boldsymbol{v}$ by DCT, the energy of interference is also equal. Then, the energy of mutual interference at the sequence $\tilde{\boldsymbol{d}}_{\boldsymbol{g}}$ is given by $\beta_u + \beta_\epsilon$ because the spectrum sequence for the embedding is equal which is related to $\boldsymbol{pn(s)}$, where β_ϵ is the energy of noise signal. If colluders are belonging to different groups, the energy at $\tilde{\boldsymbol{d}}_{\boldsymbol{u}}$ is $\beta_g + (c-1)\beta_u/c + \beta_\epsilon$ because each signal is embedded into quasi-orthogonal domain obtained by operating $\boldsymbol{pn(i_g)}$ which is related to a group ID. Our objective is to remove the interference with energy β_u for the group ID and energy $\beta_g + (c-1)\beta_u/c$ for the user ID from $\tilde{\boldsymbol{v}} - \boldsymbol{v}$ as much as possible.

It is worth mentioning that the main source of interference, which is the original image, is removed at the detection because the access to it is allowed by the assumption of a fingerprinting scheme.

3.2 Removal Operation

The knowledge of fingerprinting sequences $\boldsymbol{w_g}$ and $\boldsymbol{w_u}$ enables a detector to remove the interference effectively from the detection sequences $\tilde{\boldsymbol{d}}_{\boldsymbol{g}}$ and $\tilde{\boldsymbol{d}}_{\boldsymbol{u}}$. Because once a certain group ID is detected, its signal is merely a noise for the detection of a user ID, hence it should be removed at the detection of the user

ID. Such a removal operation minimizes the effects of interference, and decreases the variance of $\tilde{\boldsymbol{d}}_{\boldsymbol{u}}$. As the results, the true-positive detection rate is increased with no sacrifice of false one.

The abstract of the detection procedure is illustrated in Fig.3. In this figure, some fingerprint signals are involved in the sequence $\tilde{\boldsymbol{v}} - \boldsymbol{v}$ with spread form, and at the first detection (detection of a group ID) two signals are found. Before the second detection, the detected signals are removed from $\tilde{\boldsymbol{v}} - \boldsymbol{v}$, which decrease the variance of noise elements. Since the detection of a user ID is performed using one of the detected group ID, the third detection is also performed with the similar procedure to the second one. In this stage, much interference from other fingerprint signals is removed, hence the number of detectable colluders is increased compared with the original method. If the detection operation is performed once again, some undetected signals at the first detection can be found because of the decrease of variances of noise elements.

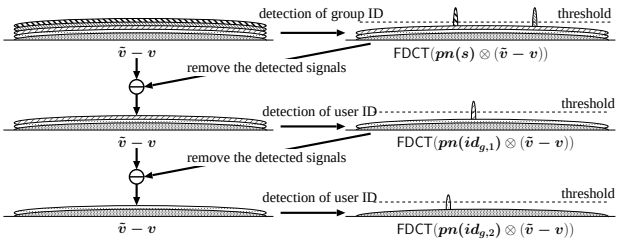

Fig. 3. Illustration of proposed detection procedure.

To implement the procedure, the proposed removal operations described below are inserted in the original detection method.

3-5. The corresponding signals of detected group IDs are removed from $\tilde{\boldsymbol{v}}$;

$$\tilde{\boldsymbol{v}} \leftarrow \tilde{\boldsymbol{v}} - \sum_{k} \boldsymbol{dct}(\boldsymbol{k}, \tilde{\boldsymbol{d}}_{\boldsymbol{g},\boldsymbol{k}}) \tag{12}$$

4-5. The corresponding signals of detected user IDs are removed from $\tilde{\boldsymbol{v}}$;

$$\tilde{\boldsymbol{v}} \leftarrow \tilde{\boldsymbol{v}} - \sum_{h} \boldsymbol{dct}(\boldsymbol{h}, \tilde{\boldsymbol{d}}_{\boldsymbol{u},\boldsymbol{h}}) \tag{13}$$

5 If at least one user ID is detected by the Step 4, go to Step 3, otherwise quit the detection operation.

As described in Step 5, the detection of a group ID and a user ID with the above removal operations are repeatedly performed when at least one user ID is detected. As the consequence, the thresholds T_g and T_u related to the variance of $\tilde{\boldsymbol{v}} - \boldsymbol{v}$ is decreased without increasing the false-positive rate seriously.

3.3 Two kinds of Thresholds

When embedded signals as fingerprint information are successively and correctly removed during the proposed detection process, the effects of mutual interference are minimized. Due to the increase of the number of colluders, wrong signals will be accidentally detected because the effects of interference are increased with respect to the number. In such a case, the undetected fingerprint signal is attenuated by the removal operation.

Since the characteristic of a CDMA channel at the detection sequence, an interference and noise signals follow normal distribution with zero mean. Considering the effects of such signals, fingerprinted signals are also represented by normal distribution which mean is β_g/c. Based on the Eq.(7), a false-positive probability Pe_g for the detection of a group ID is represented by,

$$Pe_g = \frac{1}{2}\,\mathrm{erfc}\left(\frac{T_g}{\sqrt{2\sigma^2}}\right), \tag{14}$$

where T_g is a threshold. The expected number of wrongly detected group ID from detection sequence $\tilde{\boldsymbol{d}}_{\boldsymbol{g}}$ is calculated from the false-positive probability Pe_g and the variance σ^2 of the sequence $\tilde{\boldsymbol{d}}_{\boldsymbol{g}}$. If the length of the sequence is ℓ, the number is given by $\ell \times Pe_g$. For example, when $\ell = 1024$ and $Pe_g = 10^{-3}$, which are used in the simulation of [11], are assigned, one of the detected group ID is wrong in average. Remember that some fingerprint signals will be covered by noise signals because of the attenuation of energy after averaging collusion. For the detection of a group ID, the false-negative detection of fingerprinted signals is much serious because the following detection of the user ID is not conducted. Even if the false-positive detection of a group ID is increased, the actual false-positive detection is bounded to the detection of the user ID. Hence, it is advisable to decrease Pe_g forgiving the false detection from this point of view.

When the threshold T_g for a group ID goes down, the number of detected group ID is increased. It provides the chance for mining the corresponding user ID from a detection sequence. If all detected signals are removed as an interference, wrongly detected signals at the detection of a group ID are also removed and the detection operation is performed again with the threshold which goes down after the removal under a constantly designed false-positive rate. Hence, the repeat of detection operation provides the chance, regretfully, to detect wrong ID by mistake, which causes the increase of the false detection. So our objective is to perform the removal operation selectively for the detection signals and to omit some repetition of detection. In order not to remove too much, two kinds of thresholds T_g^L and T_g^H, $(T_g^L < T_g^H)$ for group ID are introduced. If $\tilde{d}_{g,k}$, $(0 \le k \le \ell)$ are larger than the lower threshold T_g^L, they are regarded as the candidates of colluders' group ID. Then, some of them that exceed the higher threshold T_g^H are subtracted from the detection sequence as an interference, and the others are removed only when the corresponding signals of the user ID are detected, otherwise left the signals.

Similar to the above discussion, when the threshold T_u for a user ID decreases, the number of detected user ID is also increased. In this case, however, it directly raises the false-positive detection rate. By introducing two kinds of thresholds T_u^L and T_u^H, $(T_u^L < T_u^H)$, the objective signals are detected adaptively as follows. Our detector detects some candidates of the user ID using the lower threshold T_u^L and removes these detected signals as well as the corresponding signals of the group ID. Final decision are done by the threshold T_u^H to exclude the false detection.

Once user IDs are found at the detection sequence $\tilde{\boldsymbol{d}}_{\boldsymbol{u}}$, the repeat of detection operation will be needless. In order not to perform again the detection operation for such a case, when at least one user corresponding to a certain group ID has already been found, the repeat of detection operation for the user ID is omitted.

Based on the above two ideas, the proposed detection procedure is described as follows.

1. Perform full-domain DCT on a pirated copy.
2. Select ℓ DCT coefficients from low- and middle-frequency domains on the basis of a secret key key, which is denoted by $\tilde{\boldsymbol{v}}$.
3. Detect group ID by the following operations.
   3-1 Generate a PN sequence $\boldsymbol{pn(s)}$ generated by a secret key s, and multiply $\tilde{\boldsymbol{v}} - \boldsymbol{v}$ to it.
   3-2 Perform 1D-DCT to obtain the detection sequence $\tilde{\boldsymbol{d}}_{\boldsymbol{g}}$;

$$\tilde{\boldsymbol{d}}_{\boldsymbol{g}} = \mathsf{FDCT}\big(\boldsymbol{pn(s)} \otimes (\tilde{\boldsymbol{v}} - \boldsymbol{v})\big). \tag{15}$$

   3-3 Calculate the variance of $\tilde{\boldsymbol{d}}_{\boldsymbol{g}}$ considering the property of its distribution and determine two thresholds T_g^H and T_g^L with a given false-positive probability Pe_g^H and Pe_g^L, respectively.
   3-4 If $\tilde{d}_{g,k} \geq T_g^L, (0 \leq k \leq \ell - 1)$, determine k as the group ID, and store the signals,

$$\hat{d}_{g,k} = \begin{cases} \tilde{d}_{g,k} & (\tilde{d}_{g,k} < T_g^H) \\ 0 & \text{otherwise.} \end{cases}$$

   3-5 If $\tilde{d}_{g,k} \geq T_g^H, (0 \leq k \leq \ell - 1)$, the corresponding signals of detected group IDs are removed from $\tilde{\boldsymbol{v}}$;

$$\tilde{\boldsymbol{v}} \leftarrow \tilde{\boldsymbol{v}} - \sum_{\tilde{d}_{g,k} \geq T_g^H} \boldsymbol{dct(k, \tilde{d}_{g,k})}. \tag{16}$$

4. Perform the following operation for each group ID if no signal has detected from the corresponding detection sequence of the user ID.
   4-1 Generate a PN sequence $\boldsymbol{pn(i_g)}$, and multiply $\tilde{\boldsymbol{v}} - \boldsymbol{v}$ to it.
   4-2 Perform 1D-DCT to obtain the detection sequence $\tilde{\boldsymbol{d}}_{\boldsymbol{u}}$;

$$\tilde{\boldsymbol{d}}_{\boldsymbol{u}} = \mathsf{FDCT}\big(\boldsymbol{pn(i_g)} \otimes (\tilde{\boldsymbol{v}} - \boldsymbol{v})\big). \tag{17}$$

4-3 Calculate the variance of $\tilde{\boldsymbol{d}}_{\boldsymbol{u}}$ and determine a lower threshold T_u^L with a given false-positive probability Pe_u^L.
4-4 If $\tilde{d}_{u,h} \geq T_u^L$, h is regarded as a candidate of the user ID i_u, and store

$$\hat{d}_{u,h} = \tilde{d}_{u,h} \tag{18}$$

as the detected signal strength for this candidate.
4-5 The corresponding signals of the candidates are removed from $\tilde{\boldsymbol{v}}$;

$$\tilde{\boldsymbol{v}} \leftarrow \tilde{\boldsymbol{v}} - \boldsymbol{dct}(\boldsymbol{k}, \hat{\boldsymbol{d}}_{\boldsymbol{g},\boldsymbol{k}}) - \sum_{h} \boldsymbol{dct}(\boldsymbol{h}, \tilde{\boldsymbol{d}}_{\boldsymbol{u},\boldsymbol{h}}). \tag{19}$$

5. At least one candidate is detected by the Step 4, go to Step 3, otherwise, go to Step 6.
6. Perform the following operation for each candidate of the user ID.
   6-1 Perform the same operations as Step 4-1 and Step 4-2.
   6-2 Calculate the variance of $\tilde{\boldsymbol{d}}_{\boldsymbol{u}}$, and determine a threshold T_u^H with a given false-positive probability Pe_u^H.
   6-3 If $\hat{d}_{u,h} + \tilde{d}_{u,h} \geq T_u^H$, determine h as the user ID i_u.

It is noticed that the final decision of detected ID is determined at Step 6. Because the detected signals of the user ID at Step 4 may contain the noise and interference of undetected signals, the decision should be done after all removal operations. The noise and interference contained in the sequence $\tilde{\boldsymbol{d}}_{\boldsymbol{u}}$ when the user ID is detected at Step 4 are represented by $\tilde{d}_{u,h}$.

4 Computer Simulated Results

For the evaluation of the proposed detection method, we implement the algorithm and compare the number of detected colluders from a pirated copy with averaging collusion. As a host signal, we use a standard image "lena" that has 256-level gray scale with a size of 512×512 pixels. In our simulation, the embedding strengths are fixed by $\beta_g = 400$ and $\beta_u = 600$, respectively. Fingerprinted images are produced by embedding 10^4 patterns of randomly selected i_g and i_u, and a pirated copy is an averaged one of them and it is compressed by JPEG algorithm with a quality factor of 35%. Then, the value of PSNR is 45 [dB]. The detection of the fingerprint is performed with the knowledge of the host image. As a comparison, the proposed detection method with the removal operation introduced in subsection 3.2 applied for the original one is called method I, and the one with two kinds of thresholds for the detection of each ID is method Ⅱ.

We explore the false-positive detection performance of our detection methods using the fingerprint sequences of length $\ell = 1024$. Thus, the allowable number of users is $1024^2 (\approx 10^6)$. As discussed in Section 3, the actual probability P_{fp} of false-positive detection is dependent on the design of Pe_g and Pe_u for method I and Pe_g^L, Pe_g^H, Pe_u^L, and Pe_u^H for method Ⅱ. The probability P_{fp} is defined as an average number of falsely detected innocent users at one detection. A threshold T

Table 1. The relations between $\overline{T}$ and a false-positive probability Pe.

Pe	5×10^{-3}	1×10^{-3}	1×10^{-4}	1×10^{-5}	1×10^{-6}	1×10^{-7}	1×10^{-8}	2.5×10^{-9}
$\overline{T}$	1.82	2.19	2.63	3.02	3.36	3.68	3.97	4.13

Table 2. The actual probability of false-positive detection for different thresholds when method I with $\ell = 1024$ is applied.

	original	method I	
$\overline{T_g}$	2.19	2.19	1.82
$\overline{T_u}$	3.97	3.97	3.97
P_{fp} $[\times 10^{-4}]$	2.00	2.63	17.46

Table 3. The actual probability of false-positive detection for different thresholds when method II with $\ell = 1024$ is applied.

	method II								
type	i	ii	iii	iv	v	vi	vii	$viii$	ix
$\overline{T_g^L}$	1.82			1.82			1.82		
$\overline{T_g^H}$	2.19			2.63			2.63		
$\overline{T_u^L}$	3.97	3.68	3.36	3.97	3.68	3.36	3.36	3.02	2.63
$\overline{T_u^H}$	3.97			3.97			4.13		
P_{fp} $[\times 10^{-4}]$	3.00	6.29	8.75	2.38	4.75	6.33	2.21	3.04	11.08

of a false-positive probability Pe is given by Eq.(7), and the relation is simplified by

$$T = \overline{T} \times \sqrt{2\sigma^2}, \tag{20}$$

where $\overline{T}$ is the relevant variable. Some values used in our simulation are listed at Table 1, and the false-positive probabilities using method I are at Table 2. It is confirmed that the probability P_{fp} is increased if $\overline{T_g}$ goes down. Table 3 shows the probabilities of method II for 9 types of thresholds considering the probability P_{fp}. Due to the precision of P_{fp} in our simulation, the probabilities in the table are the average number of falsely detected innocent users with the number of colluders from 7 to 40. Considering the size of P_{fp}, the number of detected colluders with original method, method I using $\overline{T_g} = 2.19$ and $\overline{T_u} = 3.97$, and method II of type i, iv, vii, and $viii$ are plotted in Fig. 4. The effectiveness of removal operations introduced in method I is confirmed, and using two kinds of thresholds at each level of detection the performance can be improved. Considering the trade-off between the number of detected colluders and the false-positive probability, the method II with type $viii$ holds a better performance. Hereafter, we simply denote the method with these specific parameters by proposed I and proposed II.

If ℓ is doubled, the false-positive probability also becomes double because the probability is proportionally increased by the number. For the evaluation of the

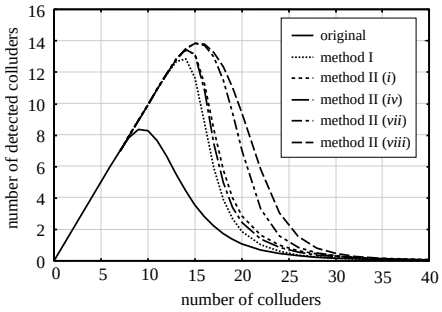

Fig. 4. The comparison of the number of detected colluders with $\ell = 1024$ for an image "lena".

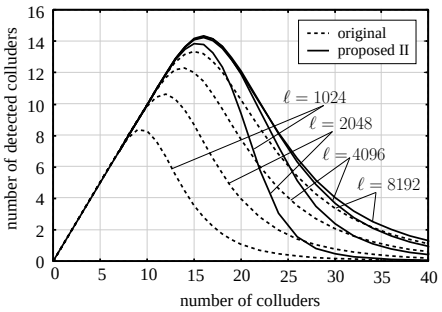

Fig. 5. The number of detected colluders for an image "lena".

true-positive detection of proposed Ⅱ under an equal condition, the number of users is fixed to $2^{20}(= 1024 \times 1024)$ for different ℓ. The results for different length $\ell = 1024, 2048, 4096, 8192$ are plotted in Fig.5, and the actual probabilities of false detection are shown in Table 4. Since a short sequence is more volunerble to the interference of noise elements such as JPEG compression, P_{fp} of length $\ell = 1024$ is degraded. The false-negative rate, which is the error rate of catching no colluder, is also evaluated for proposed Ⅱ, and the results are plotted in Fig.6. The results of other images with $\ell = 8192$ are shown in Fig.7, Fig.8, and Table 5. These results confirm that the proposed detection method can catch more colluders and less innocent users with high probability.

It is worth mentioning that the proposed removal operation is applicable to the conventional spread spectrum watermarking scheme [3]. However, considering the computational complexity required for the iterative detection procedure, the CDMA-based fingerprinting scheme is suitable to implement.

Table 4. The probability of false-positive detection for an image "lena".

	P_{fp} $[\times 10^{-4}]$		
ℓ	original	proposed Ⅰ	proposed Ⅱ
1024	2.00	2.63	3.04
2048	2.08	3.08	1.08
4096	1.54	3.17	1.08
8192	3.83	4.38	1.58

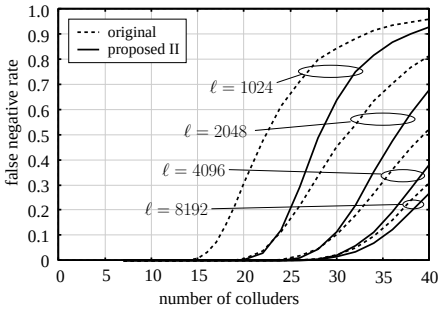

Fig. 6. The false-negative detection rate for an image "lena".

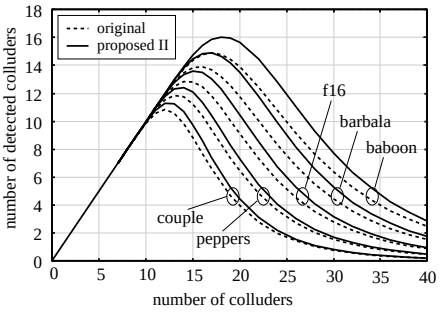

Fig. 7. The number of detected colluders for some images with $\ell = 8192$.

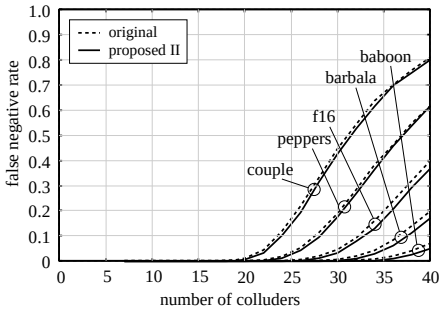

Fig. 8. The false-negative detection rate for some images with $\ell = 8192$.

Table 5. The probability of false-positive detection for some images with $\ell = 8192$.

	P_{fp} [$\times 10^{-4}$]	
	original	proposed Ⅱ
baboon	4.92	1.21
barbala	3.54	0.75
couple	3.13	1.21
f16	2.83	0.67
peppers	3.00	1.25

5 Concluding Remarks

In this paper, we proposed an effective detection method for the CDMA-based fingerprinting scheme. The model of the fingerprinting scheme gives us the way to attenuate the effects of a noise involved in detection sequences, which is a removal operation. The proposed removal operation implies that the detected signals are extracted from the detection sequence. We analyzed the effects of the removal operation on the detector, and introduced two kinds of thresholds. The detected signals of the group ID which exceed the higher threshold T_g^H are extracted from the detection sequence by a removal operation. The other detected signals which exceed the lower threshold T_g^L are removed when the corresponding user ID are detected using the lower threshold T_u^L, otherwise left the signals which are regarded as the interference of other undetected fingerprints. The final decision is done by the higher threshold T_u^H. From our simulation results, we found that the threshold T_g^H should be designed appropriately large in order not to remove undetected fingerprint signals. However, we have to remind that larger threshold T_g^H fails to remove the interference at the detection of the group ID, hence the

detection of a user ID is missed because of the remained interference. By going down the threshold T_u^L, we collect more user ID as the candidates. Since the design of thresholds is dependent on the length of spread spectrum sequence, the determination of best parameters are left for our future work.

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. Wu, M., Trappe, W., Wang, Z., Liu, K.J.R.: Collusion resistant fingerprinting for multimedia. IEEE Signal Processing Mag. (2004) 15–27
2. Pfitzmann, B., Schunter, M.: Asymmetric fingerprinting. In: EUROCRYPT'96,. Volume 1070 of LNCS., Springer, Heidelberg (1996) 84–95
3. Cox, I., Kilian, J., Leighton, F., Shamson, T.: Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Process. **6**(5) (1997) 1673–1687
4. Zhao, H., Wu, M., Wang, Z., Liu, K.J.R.: Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting. IEEE Trans. Image Process. **14**(5) (2005) 646–661
5. Wang, Z.J., Wu, M., Trappe, W., Liu, K.J.R.: Group-oriented fingerprinting for multimedia forensics. EURASIP J. Appl. Signal Process. (14) (2004) 2142–2162
6. Wang, Z.J., Wu, M., Zhao, H., Trappe, W., Liu, K.J.R.: Anti-collusion forensics of multimedia fingerprinting using orthogonal modulatio. IEEE Trans. Image Process. **14**(6) (2005) 804–821
7. Boneh, D., Shaw, J.: Collusion-secure fingerprinting for digital data. IEEE Trans. Inform. Theory **44**(5) (1998) 1897–1905
8. Trappe, W., Wu, M., Wang, Z.J., Liu, K.J.R.: Anti-collusion fingerprinting for multimedia. IEEE Trans. Signal Process. **51**(4) (2003) 1069–1087
9. Y. Zhu, D.F., Zou, W.: Collusion secure convolutional spread spectrum fingerprinting. In: IWDW 2005. Volume 3710 of LNCS., Springer, Heidelberg (2005) 67–83
10. Tardos, G.: Optimal probabilistic fingerprint codes. In: Proc. 35th ACM Symp. Theory of Comp. (2003) 116–125
11. Hayashi, N., Kuribayashi, M., Morii, M.: Collusion-resistant fingerprinting scheme based on the CDMA-technique. In: IWSEC 2007. Volume 4752 of LNCS., Springer, Heidelberg (2007) 28–43
12. Gold, R.: Maximal recursive sequences with 3-valued recursive cross-correlation functions. IEEE Trans. Infom. Theory **14**(1) (1968) 154–156
13. Stone, H.: Analysis of attacks on image watermarks with randomized coefficients. NEC Res. Inst., Tech. Rep. **96–045** (1996)
14. Rao, K.R., Yip, P.: Discrete Cosine Transform: Algorithms, Advantages, Applications. Academic Press Boston (1990)
15. Barni, M., Bartolini, F., Piva, A.: Improved wavelet-based watermarking through pixel-wise masking. IEEE Trans. on Image Process. **10**(5) (2001) 783–791