ADAPTIVE ITERATIVE DETECTION METHOD FOR SPREAD SPECTRUM FINGERPRINTING SCHEME

Minoru Kuribayashi

Graduate School of Engineering, Kobe University,
1-1, Rokkodai-cho, Nada-ku, Kobe, 657-8501 Japan.
E-mail: kminoru@kobe-u.ac.jp

ABSTRACT

The traceability of the spread spectrum fingerprinting has been improved by an iterative detection method combined with an interference removal operation. However, the false-positive probability is slightly increased when the length of fingerprint sequence is rather small. In this study, the iterative detection procedure is adaptively calibrated to maximize the effect of the interference removal operation.

Index Terms— fingerprinting, spread spectrum, interference removal operation

1. INTRODUCTION

The idea of spread spectrum fingerprinting has been proposed by Cox et al. [1] such that mutually (quasi-)orthogonal sequences are assigned to users as their fingerprints. Because of the (quasi-)orthogonality, it is possible to identify illegal users involved in a pirated copy even if they delete/alter the embedded signals by comparing the difference among their marked copies. It is reported in [2] that the spread spectrum fingerprinting scheme is argued to be highly resistant to collusion attack and it can be scaled up to hold millions of users.

In order to accommodate millions of users, quasi-orthogonal sequences must be required because the number of orthogonal sequences is just equal to the length of these sequences. However, the computational complexity at the detection increases linearly with the number of users. In order to reduce the complexity, the idea of grouping users was introduced by Wang et al. [3], and is systematically implemented in [4] using the hierarchical structure. The independency between groups limits the amount of innocent users falsely placed under suspicion within a group. Since the operation of detecting users is conducted only for the users within the groups judged suspicion, most of the operation can be cut down in the group-based scheme.

According to the increase of the users in a fingerprinting system, the mutual interference among these sequences becomes non-negligible at the detection of fingerprints. It is noticed that detected signals are assumed as the interference of other undetected signals. In [5], once a fingerprint signal is detected, the signal is removed from the detection sequence for the reduction of the interference. By iteratively performing the detecting operation combined with the removal operation, the detector can catch more colluders. Furthermore, two types of thresholds are introduced to conduct a successive removal operation in the iterative procedure. Although these thresholds are designed to control the false-positive probability, the experimental results shows that the probability is much higher than the targeted one when the length of the fingerprint sequences are small.

In this study, the interference removal operation is further optimized to reduce the false-positive probability. We present three ideas for the optimization: 1) the removal operation is repeatedly performed at each loop, 2) the detection of users within a suspicious group is performed adaptively, and 3) suspicious groups as well as suspicious users are checked at the final decision, which are checked only suspicious users in the previous method.

2. PRELIMINARIES

2.1. Spread Spectrum Watermarking

In Cox's scheme [1], a spread spectrum sequence following an i.i.d. Gaussian distribution with zero mean and variance 1, $N(0,1)$, is embedded into the frequency components of a digital image. In [4], a spread spectrum sequence is a DCT basic vector modulated by a PN-sequence. With the assist of the fast DCT algorithm, the amount of computations is reduced by a log order.

Let $\boldsymbol{v} = \{v_0, \ldots, v_{\ell-1}\}$ be the frequency components of a digital image and $\boldsymbol{w} = \{w_0, \ldots, w_{\ell-1}\}$ be the fingerprint sequence which an energy is $\beta^2 = \sum_{t=0}^{\ell-1} w_t^2$. We insert $\boldsymbol{w}$ into $\boldsymbol{v}$ to obtain a watermarked sequence $\boldsymbol{v}^*$. Specifically, we call *additive* when $\boldsymbol{v}^* = \boldsymbol{v} + \boldsymbol{w}$, and *multiplicative* when $\boldsymbol{v}^* = \boldsymbol{v}(1 + \boldsymbol{w})$. Due to the simplicity, the additive method is mainly discussed in this paper.

At the detector side, we determine which sequences are present in a pirated copy by evaluating the similarity of sequences. When a sequence $\tilde{\boldsymbol{w}}$ is extracted by calculating the difference between an original copy and pirated one, and its correlation with $\boldsymbol{w}$ is measured. If the value exceeds a threshold, the embedded sequence is regarded as $\boldsymbol{w}$.

2.2. Grouping

We assume that the number of groups is ℓ and that of users in individual group is also ℓ for simplicity. Thus, the total number of users is $\ell \times \ell$. The fingerprint sequence $\boldsymbol{w}^{(i,j)}$ assigned to the j-th user within the i-th group consists of two components.

$$\boldsymbol{w}^{(i,j)} = \boldsymbol{w}_{\boldsymbol{g}}^{(i)} + \boldsymbol{w}_{\boldsymbol{u}}^{(i,j)}, \tag{1}$$

where $\boldsymbol{w}_{\boldsymbol{g}}^{(i)}$ is the spread spectrum sequence for the i-th group and $\boldsymbol{w}_{\boldsymbol{u}}^{(i,j)}$ is that for the j-th user. Because of the presence of the common vector $\boldsymbol{w}_{\boldsymbol{g}}^{(i)}$, when colluders from the same group average their copies, the energy of the vector is not attenuated; hence, the detector can accurately identify the group. The detection algorithm consists of two stages; one involves the identification of groups containing colluders, and the other, the identification of colluders within each suspicious group.

2.3. Iterative Detection

When c colluders make a pirated copy by averaging c copies, the sequence $\boldsymbol{w'}$ extracted from the copy is represented by

$$\boldsymbol{w'} = \frac{1}{c} \sum_{(i',j') \in \mathcal{C}} \boldsymbol{w}^{(\boldsymbol{i'},\boldsymbol{j'})} + \boldsymbol{\gamma}, \tag{2}$$

where $\mathcal{C}$ is the set of colluders and $\boldsymbol{\gamma}$ is an additive noise following an i.i.d. Gaussian distribution with zero mean. In this model, c and $\boldsymbol{\gamma}$ are unknown parameters at the detector side. Suppose that $d_g^{(i')}$, and $d_u^{(i',j')}$ are the correlation values for group ID and user ID, respectively. If the fingerprint sequences are mutually orthogonal and no noise is added, $d_g^{(i')} = d_u^{(j')} = 1/c$ and Eq.(2) can be rewritten by

$$\boldsymbol{w'} = \sum_{i' \in \mathcal{G}} d_g^{(i')} \boldsymbol{w}_{\boldsymbol{g}}^{\boldsymbol{i'}} + \sum_{(i',j') \in \mathcal{C}} d_u^{(i',j')} \boldsymbol{w}_{\boldsymbol{u}}^{(\boldsymbol{i'},\boldsymbol{j'})}, \tag{3}$$

where $\mathcal{G}$ is a set of groups in which colluders involved.

Regretfully, we use quasi-orthogonal sequences, and hence, $d_g^{(i')}$ and $d_u^{(i',j')}$ involve interference terms even in a noiseless case. Because once a group ID is detected, its signal is merely a noise for the detection of user ID, hence it should be removed before the detection of user ID. Such a removal operation can be performed at each detection of user ID corresponding to groups judged suspicious. In [5], the removal operation is performed sequentially for the detected signals and the detection procedure using removal operation is performed iteratively.

The removal operation for group ID is denoted by

$$\mathsf{RMg}\big(\boldsymbol{w'}, i', d_g^{(i')}\big) : \boldsymbol{w'} \leftarrow \boldsymbol{w'} - d_g^{(i')} \boldsymbol{w}_{\boldsymbol{g}}^{(\boldsymbol{i'})} \tag{4}$$

and the removal operation for user ID is denoted by

$$\mathsf{RMu}\big(\boldsymbol{w'}, i', j', d_u^{(i',j')}\big) : \boldsymbol{w'} \leftarrow \boldsymbol{w'} - d_u^{(i',j')} \boldsymbol{w}_{\boldsymbol{u}}^{(\boldsymbol{i'},\boldsymbol{j'})} \tag{5}$$

For the detection of group ID, the false-negative detection of fingerprinted signals is a serious issue because the subsequent detection of user ID is not conducted. Even if the false-positive detection of group ID is increased, the actual false-positive detection is bounded at the detection of the user ID. When a threshold for detecting group ID goes down, the number of detected group ID is increased. It provides an opportunity for mining the corresponding user ID from a detection sequence. If all the detected signals are removed as interference, wrongly detected signals at the detection of group ID are also removed and the detection operation is performed again with the decreased threshold after removal under a constantly designed false-positive rate. Hence, repeating the detection operation provides an undesirable opportunity to detect wrong ID erroneously, which causes an increase of the false detection. In order not to remove too much, two types of thresholds both for group ID and user ID are introduced [5].

From the statistical property, if a threshold T and the variance σ^2 of the correlation scores are given, a false-positive probability ϵ is calculated by the equation

$$\epsilon = \frac{1}{2} \mathrm{erfc}\left(\frac{T}{\sqrt{2\sigma^2}} \right), \tag{6}$$

where $\mathrm{erfc}()$ is the complementary error function. Conversely, the threshold T can be calculated from σ^2 and ϵ:

$$T = \sqrt{2\sigma^2} \mathrm{erfc}^{-1}(2\epsilon). \tag{7}$$

The total false-positive probability η, that is, the probability of accusing any innocent users, is dependent on the number of the operations for detecting user ID. When the designed probability is ϵ and the number of operations is θ,

$$\eta = 1 - (1 - \epsilon)^{\ell\theta} \approx \epsilon\ell\theta. \tag{8}$$

A drawback in the previous detector is that the false-positive probability becomes considerably high when the length of fingerprint sequences are small. The main reason comes from the removal operation for wrongly detected signals.

3. PROPOSED METHOD

It is evident that the removal operation at an early stage does not sufficiently remove the fingerprint sequence involved in $\boldsymbol{w'}$ because $d_g^{(i')}$ and $d_u^{(i',j')}$ involve considerable noise due to the mutual interference among fingerprints. In order to minimize the interference as far as possible, we perform the removal operation using the re-calculated $d_g^{(i')}$ and $d_u^{(i',j')}$ for all previously detected IDs at every loop. Such operations are appeared in Steps 2-2 and 3-2 in the detection procedure described below.

Once user IDs are identified, the detection operation for this sequence need not be repeated. In order to avoid the detection operation for such a case, when at least one user

corresponding to a group ID has already been identified, the detection operation for the user ID is not repeated in the previous method. However, if the detected user ID is wrong by mistake, the detection of user ID for the corresponding group ID should be performed again, which is appeared in Step 5 described below. Fortunately, the wrongly detected IDs are excluded with high probability by the repeatedly performed removal operation because the detected signal will decreased at the final decision stage. The above detecting operations are performed adaptively using two kinds of thresholds T_g^H and T_g^L for group ID and T_u^H and T_u^L for user ID similar to the previous detector [5].

Let $\mathcal{G}'$ be a set of temporal suspicious groups and $\mathcal{G}''$ be a set of determined guilty groups. $\mathcal{C}'$ is a list of guilty users. At the initial stage, $\mathcal{G}'$, $\mathcal{G}''$, and $\mathcal{C}'$ are empty sets. For convenience, we prepare parameters $\theta = 0$, $\tilde{d}_g^{(i')} = 0$, and $\tilde{d}_u^{(i',j')} = 0$ for $0 \le i', j' \le \ell - 1$. The procedure for detecting colluders is described as follows.

1) Extract $\boldsymbol{w'}$ from a pirated copy.
2) Perform the following operations for the detection of group ID.
   2-1) Calculate the correlation values $d_g^{(i')} (0 \le i' \le \ell - 1)$ and their variance σ_g^2.
   2-2) For $i' \in \mathcal{G}''$, perform $\mathsf{RMg}\big(\boldsymbol{w'}, i', d_g^{(i')}\big)$. Add $d_g^{(i')}$ to the stored value $\tilde{d}_g^{(i')}$:
   $$\tilde{d}_g^{(i')} \leftarrow \tilde{d}_g^{(i')} + d_g^{(i')}, \tag{9}$$
   and reset the values $d_g^{(i')} = 0$.
   2-3) Determine the thresholds $T_g^H = \sqrt{2\sigma_g^2}\mathrm{erfc}^{-1}(2\epsilon_g^H)$ and $T_g^L = \sqrt{2\sigma_g^2}\mathrm{erfc}^{-1}(2\epsilon_g^L)$ using σ_g^2 and the false-positive probabilities ϵ_g^H and ϵ_g^L, respectively.
   2-4) For $i' \notin \mathcal{G}''$, if $d'_g \ge T_g^L$, add i' to the set $\mathcal{G}'$.
   2-5) Among i' added in Step 2-4, if $d_g^{(i')} \ge T_g^H$, add i' to the set $\mathcal{G}''$ and perform $\mathsf{RMg}\big(\boldsymbol{w'}, i', d_g^{(i')}\big)$; otherwise, store the correlation value in $\tilde{d}_g^{(i')}$:
   $$\tilde{d}_g^{(i')} = d_g^{(i')}. \tag{10}$$
3) Perform the following operations for $i' \in \mathcal{G}'$.
   3-1) Calculate the correlation values $d_u^{(i',j')} (0 \le j' \le \ell - 1)$ and their variance σ_u^2.
   3-2) For $(i', j') \in \mathcal{C}'$, perform $\mathsf{RMu}\big(\boldsymbol{w'}, i', j', d_u^{(i',j')}\big)$. Add $d_u^{(i',j')}$ to the stored value $\tilde{d}_u^{(i',j')}$:
   $$\tilde{d}_u^{(i',j')} \leftarrow \tilde{d}_u^{(i',j')} + d_u^{(i',j')}, \tag{11}$$
   and reset the values $d_u^{(i',j')} = 0$.
   3-3) Determine the threshold $T_u^L = \sqrt{2\sigma_u^2}\mathrm{erfc}^{-1}(2\epsilon_u^L)$ using σ_u^2 and the false-positive probability ϵ_u^L.
   3-4) For $(i', j') \notin \mathcal{C}'$, if $d'_u \ge T_u^L$, add (i', j') to the set $\mathcal{C}'$ and perform $\mathsf{RMu}\big(\boldsymbol{w'}, i', j', d_u^{(i',j')}\big)$. Store the correlation value in $\tilde{d}_u^{(i',j')}$:
   $$\tilde{d}_u^{(i',j')} = d_u^{(i',j')}, \tag{12}$$
   and increment $\theta \leftarrow \theta + 1$.
   3-5) Among (i', j') added in Step 3-4, if $i' \notin \mathcal{G}''$, perform $\mathsf{RMg}\big(\boldsymbol{w'}, i', d_g^{(i')}\big)$ and reset the stored value $d'_g = 0$.
4) If at least one candidate is detected in Step 3, go to Step 2; otherwise, go to Step 5.
5) For $(i', j') \in \mathcal{C}'$, perform the following operations.
   5-1) Calculate the correlation values $d_u^{(i',j')} (0 \le j' \le \ell - 1)$ and their variance σ_u^2.
   5-2) For $(i', j') \in \mathcal{C}'$, perform $\mathsf{RMu}\big(\boldsymbol{w'}, i', j', d_u^{(i',j')}\big)$. Add $d_u^{(i',j')}$ to the stored value $\tilde{d}_u^{(i',j')}$:
   $$\tilde{d}_u^{(i',j')} \leftarrow \tilde{d}_u^{(i',j')} + d_u^{(i',j')}, \tag{13}$$
   and reset the values $d_u^{(i',j')} = 0$.
   5-3) Determine the threshold T_u^L using σ_u^2 and the false-positive probability ϵ_u^L.
   5-4) For $(i', j') \notin \mathcal{C}'$, if $d'_u \ge T_u^L$, add (i', j') to the set $\mathcal{C}'$ and perform $\mathsf{RMu}\big(\boldsymbol{w'}, i', j', d_u^{(i',j')}\big)$. Store the correlation value in $\tilde{d}_u^{(i',j')}$:
   $$\tilde{d}_u^{(i',j')} = d_u^{(i',j')}, \tag{14}$$
   and increment $\theta \leftarrow \theta + 1$.
6) For $(i', j') \in \mathcal{C}'$, perform the following operations.
   6-1) Calculate the correlation values $d_u^{(i',j')} (0 \le j' \le \ell - 1)$ and their variance σ_u^2.
   6-2) Determine the higher thresholds T_g^H and T_u^H using σ_u^2 and the false-positive probabilities ϵ_g^H and $\epsilon_u^H = \eta/\ell\theta$, respectively.
   6-3) If $\tilde{d}_g^{(i')} < T_g^H$ or $\tilde{d}_u^{(i',j')} + d_u^{(i',j')} < T_u^H$, remove (i', j') from the set $\mathcal{C}'$.
7) Output $\mathcal{C}'$ as a set of colluders' fingerprint information.

In order to avoid the false-positive detection as far as possible, the stored correlation values $\tilde{d}_g^{(i')}$ and $\tilde{d}_u^{(i',j')}$ are checked in Step 6-3 whether they exceed the higher thresholds T_g^H and T_u^H in the proposed detector, while only $\tilde{d}_u^{(i',j')}$ is checked in the previous detector. For comparison, we implement the proposed detector without the check of $\tilde{d}_g^{(i')}$, which is called "proposed I", and the detector described above is called "proposed II".

Table 1. Designed probabilities.

ϵ_g^L	ϵ_g^H	ϵ_u^L	η
0.5×10^{-3}	10^{-4}	10^{-5}	10^{-4}

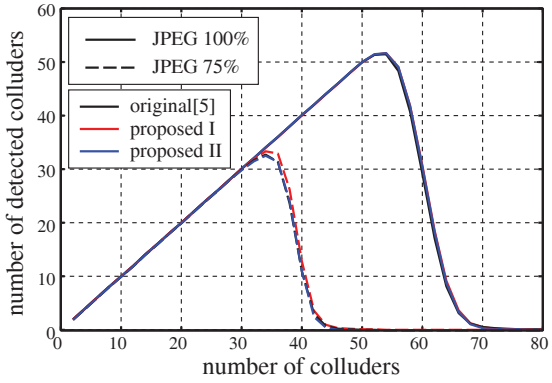


Fig. 1. Comparison of the number of detected colluders.

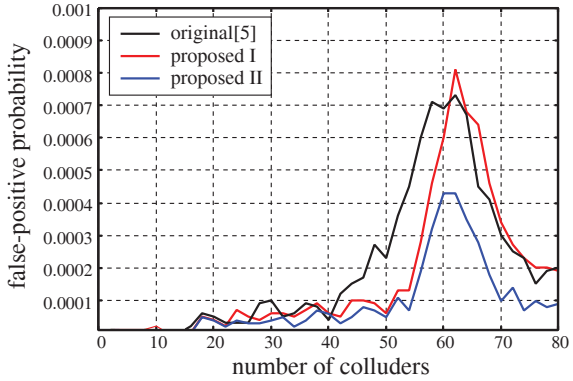
4. SIMULATION RESULTS

We use a standard image "lena" which has 256-level gray scale with a size of 512×512 pixels. The same embedding strengths in [4] are used in this experiment. Then, the average value of PSNR is 45 [dB]. The length of fingerprint sequence is $\ell = 1024$ and the number of users is 2^{20} (1024 groups $\times$ 1024 users per group). The total false-positive probability is fixed to $\eta = 10^{-4}$ using the given parameters ϵ_g^L, ϵ_g^H, and ϵ_u^L as shown in Table 1, which are the same probabilities in [5]. Randomly selected $c (2 \leq c \leq 80)$ copies are averaged, and their fingerprints are detected. This trial is performed 10^5 times.

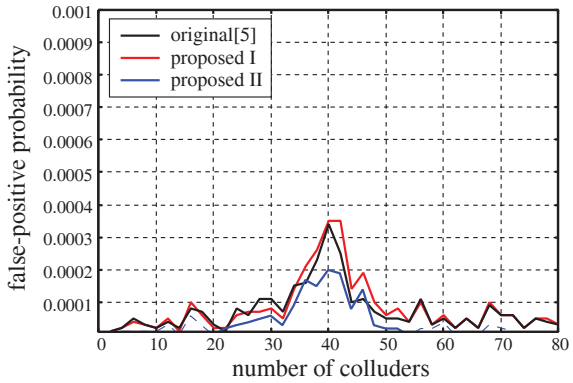
The number of detected colluders against the averaging collusion and the JPEG compression is shown in Fig. 1, and its false-positive probability is shown in Fig. 2. It is observed that the performance of proposed I is slightly better than that of original method. The false-positive probability of proposed I becomes lower though the peak is slightly increased. On the other hand, although the traceability of proposed Ⅱ is almost equal to that of original method, the false-positive probability is significantly decreased.

5. CONCLUSION

In this paper, we proposed an adaptive removal operation for the CDMA-based fingerprinting scheme. The proposed detector iteratively performs a detecting operation and sequentially reduces the interference amonog fingerprints. From the experimental results, it is confirmed that the false-positive probability can be reduced when the interference among fingerprints are relatively large.



(a) JPEG 100%



(b) JPEG 75 %

Fig. 2. Comparison of the probability of false-positive.

6. REFERENCES

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

[2] S. He and M. Wu, "Collusion-resistant video fingerprintingfor large user group," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 4, pp. 697–709, 2007.

[3] Z. J. Wang, M. Wu, W. Trappe, and K. J. R. Liu, "Group-oriented fingerprinting for multimedia forensics," *EURASIP J. Appl. Signal Process.*, , no. 14, pp. 2142–2162, 2004.

[4] M. Kuribayashi, "Hierarchical spread spectrum fingerprinting scheme based on the cdma technique," *EURASIP J. Inform. Security.*, , no. 502782, pp. 16, 2011.

[5] M. Kuribayashi, "Interference removal operation for spread spectrum fingerprinting scheme," *IEEE Trans. Inf. Forensics Security*, (accepted).