DOI: 10.3745/KIPSTD.2008.15-D.5.713

선형결합 공모공격에 강인한 각도해석 기반의 대용량 핑거프린팅

설 재 민[†] · 김 성 환[††]

요 약

핑거프린팅이란 허가되지 않았거나 불법적인 사본의 출처를 확인하기 위해, 사용자마다 개별적인 워터마크를 삽입하는 기술이다. 공모공격이란 다수의 사용자가 공모하여, 개별적인 워터마크가 삽입된 사본의 평균값이나 중앙값을 이용함으로써 공모자의 식별을 방해하는 경우이며, 개별적인 워터마크는 공모방지코드 (anti-collusion Code: ACC)를 사용하여 표시하게 된다. 하지만 공모방지코드는 평균화 공격과 중앙값 공격에 강인성을 보이지만, 선형결합공모공격 (Linear Combination Collusion Attack: LCCA)에 취약하며, 많은 수의 사용자를 지원하지 못하는 단점이 있다. 본 논문에서는 많은 수의 사용자를 지원하고, 선형결합공모공격에 견고한, 가변공모방지코드 (Scalable ACC)와 각도해석전략 (Angular Decoding Strategy)을 제안하였다. 기존의 공모방지코드에 정규분포를 가지는 확률변수를 결합하여 평균과 중앙값 공격에 강인한 가변공모방지코드를 설계하였고, 인간의 시각적 특성을 이용한 워터마킹 방법을 사용하여 핑거프린트를 영상에 삽입하였다. 공모공격에 대한 강인성을 비교하기 위해, 표준실험영상 실험 결과, 본 논문에서 제안하는 방법은 평균 및 중앙값 공격에 대하여 공모자 추적 능력이 우수하였으며, 특히 많은 사용자 중에서 다수의 공모자가 선형결합공모공격을 이용하여 공모하는 경우, 높은 공모추적 성능을 보였다.

키워드 : 디지털 핑거프린팅, 공모방지코드, 각도해석, BIBD

Scalable Fingerprinting Scheme based on Angular Decoding for LCCA Resilience

Jae Min Seol[†] · Seong Whan Kim[††]

ABSTRACT

Fingerprinting scheme uses digital watermarks to trace originator of unauthorized or pirated copies, however, multiple users may collude and escape identification by creating an average or median of their individually watermarked copies. Previous research works are based on ACC (anti-collusion code) for identifying each user, however, ACC are shown to be resilient to average and median attacks, but not to LCCA and cannot support large number of users. In this paper, we propose a practical SACC (scalable anti-collusion code) scheme and its angular decoding strategy to support a large number of users from basic ACC (anti-collusion code) with LCCA (linear combination collusion attack) robustness. To make a scalable ACC, we designed a scalable extension of ACC codebook using a Gaussian distributed random variable, and embedded the resulting fingerprint using human visual system based watermarking scheme. We experimented with standard test images for colluder identification performance, and our scheme shows good performance over average and median attacks. Our angular decoding strategy shows performance gain over previous decoding scheme on LCCA colluder set identification among large population.

Keywords : Digital Fingerprinting, Anti-Collusion Code, Angular Decoding, BIBD

1. Introduction

A digital watermark is an invisible mark inserted in digital media, and fingerprinting uses digital watermark to determine originators of unauthorized/pirated copies. Multiple users may collude and collectively escape identification by creating an average or median of their individually watermarked copies. We can think fingerprints as a palette. A palette has n color inks, and each color represent individual fingerprint signal. If a color is not the color, which already in the palette, the color must be mixed from of some color inks

※ All the correspondence should be directed to Seong-Whan Kim (corresponding author: swkim7@uos.ac.kr).
† 정 회 원 : 한국전자통신연구원 연구원
†† 정 회 원 : 서울시립대학교 컴퓨터과학부 부교수
논문접수 : 2007년 7월 14일
수 정 일 : 1차 2008년 9월 8일
심사완료 : 2008년 9월 9일

in the palette. If red and blue colored users collude, the content shall be violet. Because the violet color is not in content owner's palette, red and blue colored users will be captured, however, if the violet was already in the palette, innocent user can be suspected. Boneh assumes marking assumption, which state that the colluders can compare with their copies, identify different marks, and change it. However, undetectable marks cannot be arbitrarily changed without rendering the object useless. Therefore, the undetectable marks will be clues to colluders. To put it simply, we can increase the collusion robustness as the fingerprint gets similar to each other. However, we should have more different marks to distinguish the more users.

An early work on designing collusion-resistant binary fingerprint codes for generic data was based on marking assumption, which attackers can compare values of and can even change with making un-readable different marks. However, undetectable marks cannot be arbitrarily changed without rendering the object useless. But multimedia data have very different characteristics from generic data. Therefore we can spread different marks or fingerprints in overall images, which is biased strict marking assumption. Recently, there is an improvement to merge the low level code (primitive code) with the direct sequence spread spectrum embedding for multimedia and extend the marking assumption to allow random jamming [1]. W. Trappe presented the design of collusion-resistant fingerprints using code modulation. They proposed a (k-1) collusion-resistant fingerprints scheme, and the (k-1) resilient ACC is derived from (v, k, 1) balanced incomplete block design (BIBD) [2]. The resulting (k-1) resilient ACC code vectors are v-dimensional, and can represent $n = (v^2 - v) / (k^2 - k)$ users with these v basis vectors. However, recent research shows that LCCA (linear combination collusion attack) can successfully make collusion for ACC based fingerprinting schemes [3]. In addition, ACC which derived from BIBD cannot provide flexible coding parameters for practical fingerprinting use.

We review previous approach for collision robustness in section 2, In section 3 and we present a scalable ACC fingerprinting design scheme, which extends ACC for large number of user support. We also present an improved detection scheme using the angular decoding strategy to be robust on LCCA. In section 4 we evaluate our scheme with standard test images, and show good collusion detection performance over average, median, and linear combination collusion attacks. We conclude in Section 5.

2. Related Works

An early work on designing collusion-resistant binary fingerprint codes was presented by Boneh and Shaw in 1995 [4], which primarily considered the problem of fingerprinting generic data that satisfy an underlying principle referred to as the marking assumption. A fingerprint consists of a collection of marks, which take a finite number of states. A mark is considered to be detectable when a coalition of users does not have the same mark in that position. The marking assumption states that undetectable marks cannot be arbitrarily changed without rendering the object useless; however, it is considered possible for the colluding set to change a detectable mark to any state (collusion framework). Under the collusion framework, Boneh and Shaw show that it is not possible to totally design c-secure codes, which are fingerprint codes that are capable of tracing at least one colluder out of a coalition of at most c colluders. Instead, they used hierarchical design and randomization techniques to construct c-secure codes that are able to capture one colluder out of a coalition of up to c colluders with high probability. The construction of c-secure codes involves three stages: (1) the construction of base code using primitive codes, (2) the composition of the base code with an outer code to improve the efficiency for a large number of users, and (3) repetition and permutation to hide the position of fingerprint bits.

W. Trappe presented the design of collusion-resistant fingerprints using code modulation[2]. The fingerprint signal w_j for the j^{th} user is constructed using a linear combination of a total of v orthogonal basis signals $\{u_i\}$ as equation (1) Here the coefficients $\{c_{ij}\}$, representing the fingerprint codes, are constructed by code vectors with $\{\pm 1\}$.

$$\mathbf{w}_j = \sum_{i=1}^{v} c_{ij} \cdot \mathbf{u}_i. \tag{1}$$

Anti-collusion codes can be used with code modulation to construct a family of fingerprints with the ability to identify colluders. An anti-collusion code (ACC) is a family of code vectors for which the bits shared between code vectors uniquely identifies groups of colluding users. ACC codes have the property that the composition of any subset of K or fewer code vectors is unique. This property allows for the identification of up to K colluders. A K-resilient ACC is such a code where the composition is an element- wise AND operation. It has been shown that binary-valued ACC can be constructed using balanced incomplete block design (BIBD) [5]. The definition of (v, k, λ) BIBD is a pair (x, B), where Bis a collection of k element subsets (blocks) of v element set$x$, such that each pair of element of

$x$occurs together exactly in λ blocks. [2, 5]. The (v, k, λ) BIBD has a total of n = $\lambda(v^2 - v)/(k^2 - k)$ blocks, and we can represent (v, k, λ) BIBD code using an v x n incidence matrix M, where M(i, j) is set to 1 when the i^{th} element belongs to the j^{th} block, and set to 0 otherwise. The corresponding (k−1)-resilient ACC code vectors are assigned as the bit complements (finally represented using -1 and 1 for the 0 and 1, respectively) of the columns of the incidence matrix of a (v, k, 1) BIBD. The resulting (k-1) resilient ACC code vectors are v-dimensional, and can represent n = $(v^2 - v) / (k^2 - k)$ users with these v basis vectors.

To embed fingerprinted signal into still images, we use the equation (2) where y_j is j^{th} user's fingerprinted image, X is a host image, and α is scaling factor.

$$\mathbf{y}_j = \mathbf{x} + \alpha \mathbf{w}_j \tag{2}$$

To determine who colluders are, W. Trappe used the v dimensional collusion detection vector ($\hat{\mathbf{T}}$), which is correlation between W_j and $\{\mathbf{u}_i\}$as following equation (3).

$$\hat{\mathbf{T}} = \{t_1, t_2, \cdots, t_v\} = \frac{\mathbf{w}_j \cdot \{\mathbf{u}_1, \mathbf{u}_2 \cdots, \mathbf{u}_v\}}{\sqrt{|\mathbf{w}_j|^2 \times |\mathbf{u}_i|^2}} \tag{3}$$

Next, we convert $\hat{\mathbf{T}}$ vector to binary values ($\hat{\mathbf{T}}_b$) using a predefined threshold value, which determinates detection performance. Checking the '1' position between $\hat{\mathbf{T}}_b$ and $\mathbf{c}_j$ (j^{th} user's signature), we can decide that j^{th} user is suspected to be a traitor. This collusion detection procedure (hard detection) is suggested by W. Trappe with other two detection strategies (adaptive sorting approach, sequential algorithm), however, he did not consider any detection strategies for the linear combination collusion attack [2].

The linear collusion attack is generalized by the following equation (4), where $\mathbf{z}$ denotes additive noise. If j^{th} user does not participate in collusion, the coefficient of j^{th} user will be zero ($\beta_j = 0$). There are two constraints: (1) $\sum_{j=1}^{n} \beta_j = 1$(not to decrease quality of image) and (2) if j^{th} and k^{th} users participate in collusion, $|\beta_j| \approx |\beta_k|$ (to equalize the probability of captured) [6].

$$\begin{aligned} \hat{\mathbf{y}} &= \beta_1 \mathbf{y}_1 + \beta_2 \mathbf{y}_2 + \cdots + \beta_n \mathbf{y}_n + \mathbf{z} \\ &= \sum_{j=1}^{n} \beta_j \mathbf{x} + \sum_{j=1}^{n} \beta_j \mathbf{w}_j + \mathbf{z} \end{aligned} \tag{4}$$

The anti-collusion code can be resilient to average attack, which is shown in equation (5) but not to LCCA, shown in equation(6). Y. Wu shows that a linear combination collusion attack makes the ACC vulnerable [3].

$$\hat{\mathbf{w}} = \frac{1}{k} \sum_{j \in \varphi} \mathbf{w}_j, \quad where \ |\varphi| = k \tag{5}$$

$$\hat{\mathbf{w}} = -\sum_{j \in \varphi_1} \mathbf{w}_j + \sum_{k \in \varphi_2} \mathbf{w}_k \ , where \ |\varphi_1| + 1 = |\varphi_2| \tag{6}$$

3. Scalable and LCCA Robust Fingerprint Scheme

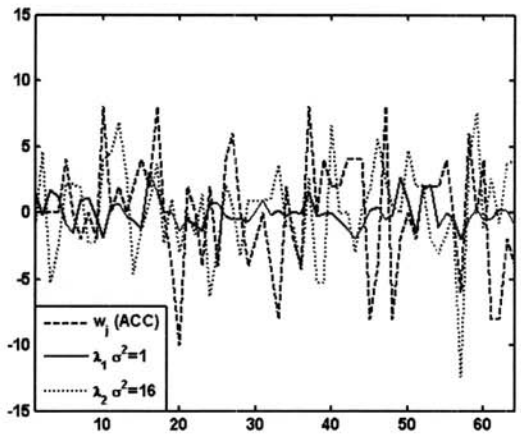
In our scheme, we construct each user's fingerprint as the composition of ACC and a Gaussian distributed random signal (lambda). Lambda means the random signal. The dimension of code vectors (M) can be increased to fit the size of fingerprinting users.

For fingerprint generation, we select one mark from M marks. The selected mark will be one of ACC, and the other marks will be lambda. For example, when the fingerprint ID is f(2,3), it means that we embed ACC #3 code in second mark, and Lambda on the other marks. Finally, the code is repeated R times and permuted. Like Boneh's scheme, the permutation sequence is unique to all users, but unknown to attackers. It also prevents interleaving collusion attack.

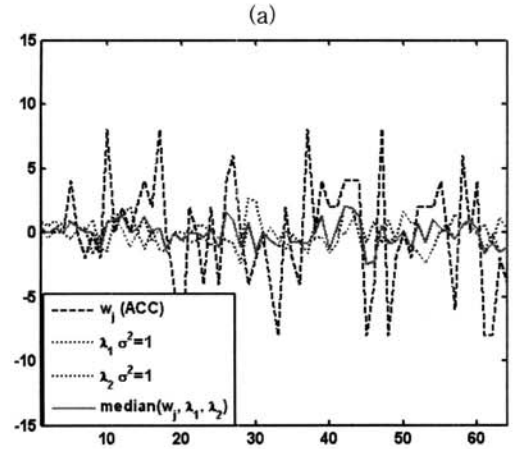
We embed fingerprint block by block basis, and we should select M times R suitable blocks to hide fingerprint signals as shown in equation (7). We exploited human visual sensitivity using noise visibility function [7, 8]. Each selected blocks are added by anti-collusion code or lambda code. Lambda code is generated using Gaussian distributed random sequence as described in [9].

$$y_k = \begin{cases} x_k + (1 - NVF) w_j, & k = 1, \cdots, M \times R \\ x_k + (1 - NVF) \lambda, & \lambda \sim N(0, \sigma^2) \end{cases} \tag{7}$$

To make scalable-ACC robust median attack, we should have lambda signal, which is similar to ACC signal and the variance of lambda is important factor; the (Figure 1(a)) shows the ACC and lambda signal. When the variance of lambda signal gets small, colluders can easily classify ACC signal and lambda signal. The easy way to classify signal is taking the median value of pixels. As shown the (Figure 1(b)), the line graph shows effect of taking median values, dashed line means ACC signal, dotted lines are lambda signal whose variance is small, and solid line represent their median values. The solid line does not have any ACC signal. Though, if the variance of lambda gets larger than ACC signals, by taking maximum or minimum values, colluders also can escape identification. From the experimentation, we heuristically set the variance



(a)



(b)

(Fig. 1) Comparison of w_j and λ value for block size = 64: (a): ACC modulated signal w_j, and two lambda signals with different variance λ_1 ($\sigma^2=1$) λ_2 ($\sigma^2=16$), (b) ACC modulated signal w_j, two small variance lambda signals λ_1 ($\sigma^2=1$) λ_2 ($\sigma^2=1$), median ($w_j, \lambda_1, \lambda_2$) signals.

of lambda to be 16 (which is equal to v parameter of BIBD code design) when we use (16, 4, 1)-BIBD code. However, lambda signal can degrade the detection precision. To achieve detection performance and median attack robustness, all signals are repeated.

For fingerprint extraction, we used non-blind scheme. For each block, we compute equation (8) and f_ks are inversely permuted.

$$f_k = \frac{y_k - x_k}{1 - NVF} \tag{8}$$

To detect colluder, we used the code matrix $\hat{\mathbf{t}}$ in equation (9), and the $\hat{t}_{m,i}$ means mth mark's averaged correlation of ith basis. The v-dimensional column vectors of T represent each mark. If the signals f_k are averaged, the variance of lambda will be decreased.

$$\hat{t}_{m,i} = \frac{1}{R}\sum_{k=1}^{R} \frac{f_{k+R(m-1)} \cdot \mathbf{u}_i}{\sqrt{|\mathbf{u}_i|^2}},\ where\ m = 1 \cdots M,\ i = 1 \cdots v \tag{9}$$

If there is no collusion, we can get either ACC or lambda, not both after extracting signals from each block (f_k). When collusion occurs, the signals will be mixed form of ACC and lambda (linear combination of ACC and lambda). However collusion occurs, the result will be complicated. But, we can use the fact that the statistics of ACC and lambda are very different. The $\hat{t}_{m,i}$ will be zero if it comes from λ because the random signal and basis are uncorrelated. To differentiate ACC modulated signal w_j and λ, we compute the score function as shown in equation (10) for each mark. If the score is small for a mark, we do not consider the mark for colluder identification because the mark is mixed signal of λ. We focus on the high scored mark $\hat{m}$ for colluder identification.

$$Score_m = -\sqrt{\sum_{i=1}^{v} t_{mi}^2} \cdot \log[P(\tau_m \mid \mu = 0)]$$
$$\hat{m} = \arg\max_{m=1 \cdots M}(score_m) \tag{10}$$

Equation (10) is composed of $\hat{t}_{m,i}$'s power and p-value. We compute $\hat{t}_{m,i}$'s power using $\sqrt{\sum_{i=1}^{v} t_{mi}^2}$, and compute the p-value $P(\tau_m|\mu=0)$, which is the probability of $\hat{t}_{m,i}$'being derived from λ, using the equation (11).

$$P(\tau_m|\mu=0) = 2\int_{\tau_m}^{\infty} \frac{\Gamma[(r+1)/2]}{\sqrt{\pi r}\Gamma[r/2]}(1+w^2/r)^{-(r+1)/2}dw,$$
$$where\ \ r = v\text{-}1,\ \tau_m = \frac{\bar{t}_m - 0}{S/\sqrt{v}},\ \bar{t}_m = \frac{1}{v}\sum_{i=1}^{v} t_{mi},$$
$$S = \frac{1}{v-1}\sum_{i=1}^{v}(t_{mi} - \bar{t})^2 \tag{11}$$

When the power is higher and $P(\tau_m|\mu=0)$ is closer to zero, the score function gets higher than others. This score function comes from the basic idea of entropy function. After we compute scores for each mark, we inspect the highest scored mark. The mark should have more evidence of colluder than low scored marks. When the mark is linear combination lambda, we assume that the mean of column vector has student T distribution with v-1 degree [10].

Without collusion attack, population of lambda is well known. However, collusion occurs, the population will be changed, and the number of colluders is not known. For instance, if we average two lambda signals whose variance

is sigma, the result will be sigma/2. However the 2 is not known to detector. But we can compute an unbiased estimator of the variance of lambda. For statistical perspective, when the variance is not known, hypothesis test on mean uses t-test with student's T distribution.

The direct sequence spreading makes collusion into linear combination of each user's fingerprint code. Mathematically, it says $\mathbf{T} = \beta_1 \mathbf{c}_{\cdot 1} + \beta_2 \mathbf{c}_{\cdot 2} + \cdots + \beta_n \mathbf{c}_{\cdot n} = \mathbf{C}\boldsymbol{\beta}$. For example, if 1st and 3rd users collude by averaging their values, the solution of $\boldsymbol{\beta}$ will be $\{1/2, 0, 1/2, 0, \cdots, 0\}$. But it is hard to estimate $\boldsymbol{\beta}$ from $\hat{\mathbf{T}}$ which is modeled as $\hat{\mathbf{T}} = \mathbf{C}\boldsymbol{\beta} + \mathbf{d}$, where $\mathbf{T}, \mathbf{d} \in R^{v \times 1}$, $\mathbf{C} \in \{-1, 1\}^{v \times n}$ and $\boldsymbol{\beta} \in R^{n \times 1}$. $\mathbf{d}$ is the processing error and noise, that can be observed at $\hat{\mathbf{T}}$. To estimate $\boldsymbol{\beta}$, we must find the following equation (12): [11, 12].

$$\min_{\boldsymbol{\beta} \in R^{n \times 1}} \left\| \hat{\mathbf{T}} - \mathbf{C}\boldsymbol{\beta} \right\|^2 \tag{12}$$

Equation (12) is called least square problem and finding exact solution is NP-hard [11]. If the $\boldsymbol{\beta}$'s domain is finite, we can use sphere decoding to solve equation (12) [12], LCCA (linear combination collusion attack) does not give change for finite domain, However we can use the singular property of (v,k,1)-BIBD, the angles between any of two user's fingerprinting code $(\mathbf{c}_{\cdot j}, \mathbf{c}_{\cdot k} \; j \neq k)$ are computed as Theorem 1.

Lemma 1. *The j^{th} block from (v, k, 1)-BIBD $\mathbf{c}_{\cdot j}$, representing j^{th} user's fingerprint code, has k elements and any two blocks (subsets) will share at most one element. Mathematically,* [2]

$$n(\mathbf{C}_j \cap \mathbf{C}_k) = 0 \; or \; 1$$

Proof: It can be derived from definition of BIBD easily. Because each pair of element of χ determines only one block, the element of intersection between arbitrary two blocks cannot exceed two.

Theorem 1. *The angle between arbitrary two users' fingerprint codes is*

$$\cos^{-1}\left(\sum_{i=1}^{v} c_{ij} c_{ik} \Big/ \left(\sqrt{\sum_{i=1}^{v} c_{ij}^2} \cdot \sqrt{\sum_{i=1}^{v} c_{ik}^2} \right) \right)$$

$$= \cos^{-1}\left(1 - \frac{4(k-1)}{v}\right) \; or \; \cos^{-1}\left(1 - \frac{4k}{v}\right)$$

Proof: We can compute $\sum_{i=1}^{v} c_{ij} \cdot c_{ik}$ by comparing the sign of each element. If i^{th} element has same sign, it will be 1 otherwise -1 (domain of $\mathbf{C}$ is $\{-1, 1\}$). Therefore,

$$\sum_{i=1}^{v} c_{ij} \cdot c_{ik} = \; \# \; of \; same \; elements - \# \; of \; different \; elements .$$

The number of different-sign elements D is $n(\mathbf{C}_i \cup \mathbf{C}_k) - n(\mathbf{C}_i \cap \mathbf{C}_k)$, and the number of same-sign elements S is $v - (n(\mathbf{C}_j \cup \mathbf{C}_k) - n(\mathbf{C}_j \cap \mathbf{C}_k))$. Using Lemma 1, we can simplify the D and S as follows.

$$\begin{aligned} D &= n(\mathbf{C}_i \cup \mathbf{C}_j) - n(\mathbf{C}_i \cap \mathbf{C}_j) \\ &= n(\mathbf{C}_i) + n(\mathbf{C}_j) - 2n(\mathbf{C}_i \cap \mathbf{C}_j) \\ &= 2(k - n(\mathbf{C}_i \cap \mathbf{C}_j)) \; = \; 2(k-1) \; or \; 2k \\ S &= the \; \# \; of \; all \; elements - D \\ &= v - 2(k-1) \; or \; v - 2k \end{aligned}$$

$$\begin{aligned} \therefore \sum_{i=1}^{v} c_{ij} c_{ik} &= \; v - 2(k-1) - 2(k-1) \; or \; v - 2k - 2k \\ &= \; v - 4(k-1) \; or \; v - 4k \end{aligned}$$

The norm of j^{th} user's fingerprint code $(\sqrt{\sum_{i=1}^{v} c_{ij}^2})$ is $\sqrt{v}$ by the definition of (v, k, 1)-BIBD ◎

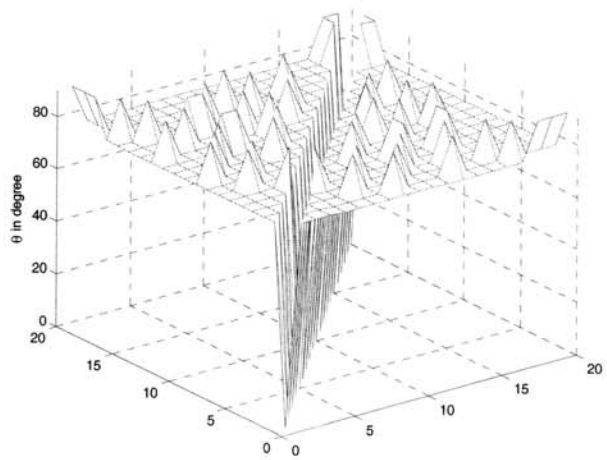
To identify colluder, we compute the angles between $\hat{\mathbf{t}}$ and each user's fingerprint codes $(\mathbf{c}_{\cdot j})$ using equation (13). If j^{th} user participates in collusion, the angle a_{jt} between j^{th} user's fingerprint code and $\hat{\mathbf{t}}$ is closer to 0 or π.

$$a_{jt} = \cos^{-1}\left(\sum_{i=1}^{v} t_{\hat{m}i} \cdot c_{ij} \Big/ \sqrt{\sum_{i=1}^{v} t_{\hat{m}i}^2 \cdot \sum_{i=1}^{v} c_{ij}^2} \right) \tag{13}$$

(Figure 2) shows that the angle between arbitrary two user's fingerprint code using (16, 4, 1)-BIBD. In this case, $\cos^{-1}(0) = 90^\circ \; or \; \cos^{-1}(1/4) = 75.5225^\circ$.

4. Analysis and Experimental Results

We experimented with the standard test images. To



(Fig. 2) Angles between each user's fingerprint code

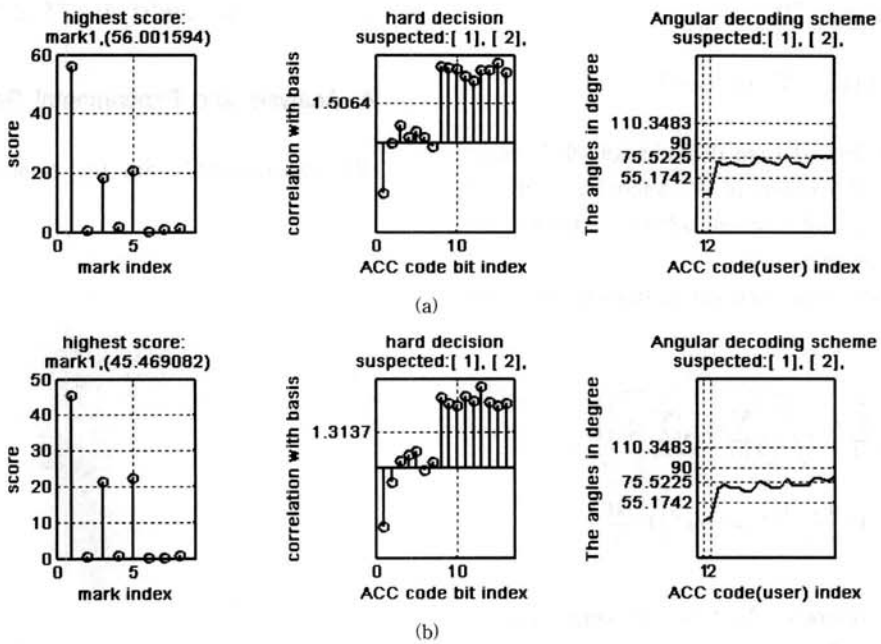
(Fig. 3) (a) Original, (b-f) five colluders' fingerprinted images, and colluded images after (g) average attack, (h) median attack, (i) LCCA

generate fingerprint signal we used (16, 4, 1)-BIBD and the Hadamard matrix whose size is 1024 (32x32) for orthogonal basis. We used $\lambda \sim N(0,4^2)$ for λ signal and we chose σ^2 as 16.0 experimentally to trade-off between median attack robustness and false positive error rate. After fingerprint embedding, the average PSNR is over 41 dB with good subjective quality.

We tested our scalable fingerprinting code for various collusion attacks (average, median, min, max, min-max, modified negative, randomized negatives and LCCA) for the test images. Taking the average of their copies is widely used as average collusion attack [13], because it is efficient to attack fingerprints, and also it makes better image quality after collusion (usually it increases 4-5 dB). (Fig. 3) shows a collusion example, when five colluders make pirated copies from their fingerprinted copies. (Figure 3) shows original image, five fingerprinted images, and colluded images after average, median, and LCCA.. As shown in (Figure 3), the average and median attacks make better image quality after collusion; however, LCCA spoils the quality of colluded image. There are many ways for collusion in LCCA, and we use the following equation for our LCCA collusion.

$$\hat{f} = -w_1\lambda\lambda\lambda\lambda\lambda - \lambda\lambda\lambda w_7\lambda + w_2\lambda\lambda\lambda\lambda\lambda + \lambda\lambda w_4\lambda\lambda\lambda + \lambda\lambda w_5\lambda\lambda\lambda$$

(Figure 4) shows the fingerprint detection result (T vectors) after average and median attack, respectively. The score results recommend that we should suspect highest scored mark #1. Next, we need to investigate 1st column of T matrix in detail. With detailed investigation, 1st and 2nd ACC codes are extracted from mark 1. After average and median attack, both angular decoding and hard decision scheme can correctly trace colluders.



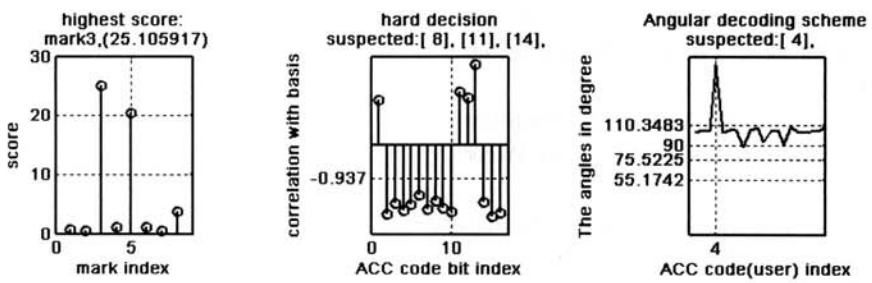
(Fig. 4) Angular decoding scheme and hard detection result:
(a) after average attack shown in Figure 3 (g), (b) after median attack shown in Figure 3 (h)

(Figure 5) shows the fingerprint detection result (T vectors) after linear combination collusion attack. After the attack, the mark #3 gets highest score, we can suspect the users in mark 3 and angular decoding scheme traces correct colluder ACC #4 in mark 3, but hard decision capture the innocent colluders. The reason why innocent users are captured is the fingerprint copy of user whose signal is acc #4 in mark 4, is negatively summed and its signal is reversed.

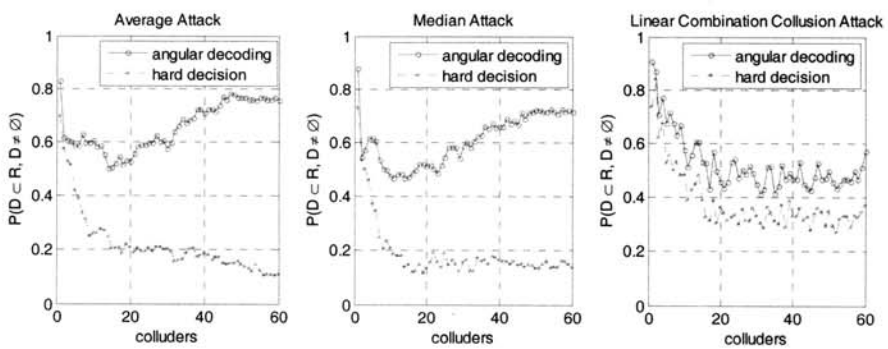
(Figure 6) show collusion performance of scalable anti-collusion code. We randomly select k colluders from 160 users, perform collusion using the k colluders, 3x3 median filter applied to remove noise and fingerprint, and finally perform detection. We iterated 200 times for each colluder selection. After detection, we compare detection result and previously selected colluders. When, the detected colluders are subset of real colluders, we considered it as success, which means that at least one colluder is captured, and there are no innocent users. The horizontal line represents the number of colluders. Y-axis represents success ratio, and, the solid line shows the angular decoding scheme and the dotted line represents hard decision. It shows that the performance of angular decoding scheme is better then hard decision scheme, under various collusion attack cases. After the LCCA, the angular decoding scheme shows better performance than hard decision scheme for large population case, because hard decision cannot set the optimal detection threshold as the number of users or colluders, whereas angular decoding exploits the knowledge of minimum angle between each users and maximize the colluder detection performance.

5. Conclusions

In this paper, we presented a scalable ACC fingerprinting scheme, which covers large number of fingerprint codes and angular decoding strategy robust to LCCA. An ACC (anti-collusion code) is hard to support large number of users (To support large users, the length of basis must be long. The longer basis is hard to hide and handle) and does not consider linear combination collusion attack. We constructed the scalable fingerprint by spreading BIBD codes over M×R (M: number of marks; R: repetition factor) image blocks. To improve the detection performance, we repeated embedding the same fingerprints over R image blocks. To increase the robustness over average and median attack, we designed a scalable ACC scheme using a Gaussian distributed random variable. We evaluated our fingerprints on standard test images, and showed good collusion detection performance over average and median collusion attacks and moderate performance over LCCA. An angular decoding strategy makes ACC invulnerable to LCCA. Although the scalability scheme makes collusion more complex and decreases detection performance of angular decoding



(Fig. 5) Angular decoding scheme and hard detection result after linear combination collusion attack shown in Figure 3 (i)



(Fig. 6) Comparison of colluder detection performance for large number of users

strategy; it can be easily controlled by the supported max users.

References

[1] Yacobi, Y., "Improved Boneh-Shaw content fingerprinting," in Proc. CTRSA2001, pp.378 - 91, 2001.

[2] Trappe, W., Wu, M., Wangm Z. J., Liu, K. J. R., "Anti-collusion fingerprinting for multimedia," IEEE Trans. Signal Proc. Vol.51, pp.1069-1087, Apr., 2003.

[3] Wu. Y., "Linear Combination Collusion Attacks and its Application on an Anti-Collusion Fingerprinting," IEEE Conf on ICASSP. Vol.51, pp.1069-1087, Apr., 2005.

[4] Boneh, D., Shaw, J., "Collusion-secure fingerprinting for digital data," IEEE Trans. Inform. Theory, Vol.44, pp.1897 -1905, Sept., 1998.

[5] Colbourn, C. J., Dinitz, J. H., "The CRC Handbook of Combinatorial Design," Boca Raton, FL: CRC Press 1996.

[6] Kundur D., Karthik K., "Video Fingerprintng and Encryption Principles for Digital Rights Management," IEEE Proc. Vol.92 pp.918-932, Jun., 2004.

[7] Voloshynovskiy, S., Herrige, A., Baumgaertner, N., Pun, T., "A stochastic approach to content adaptive digital image watermarking". Lecture Notes in Computer Science, Vol.1768, pp.211-236, Sept., 1999.

[8] Kim, S.W., Suthaharan, S., Lee, H.K., Rao, K.R., "An image watermarking scheme using visual model and BN distribution," IEE Elect. Letter, Vol.35 (3), Feb., 1999.

[9] Seol. J. M., Kim S. W., "Scalable Fingerprinting Scheme Using Statistically Secure Anti-Collusion Code for Large Scale Contents Distribution," Lecture Note on Computer Science, Vol.4906, pp560-569, Oct., 2006.

[10] Walpole R. E., Myers R. H. and Myers S. L., "Probability and Statistics for Engineers and Scientists," 6th ed, Prentice Hall, 1998

[11] Hassibi B and Vikalo H., "On the Sphere Decoding Algorithm I. Expected Complexity," IEEE trans. on signal processing Vol.53, pp.2806-2818, Aug., 2005.

[12] Li. Z. and Trappe, W., "Collusion-Resistant Fingerprinting from WBE sequence Sets" IEEE Conf. on communications, Vol.2, pp.1336-1340, May, 2005.

[13] Zhao, H., Wu, M., Wang, J., Ray Liu, K. J.: "Nonlinear collusion attacks on independent Fingerprints for multimedia" ICASSP. Vol.5, pp.664-667 Apr., 2003

설 재 민

e-mail : seoleda@gmail.com

2007년 서울시립대학교 컴퓨터통계학과 (석사)

현 재 한국전자통신연구원 연구원

관심분야 : 컴퓨터 보안, 게임기술

김 성 환

e-mail : swkim7@uos.ac.kr

1999년 한국과학기술원 전자전산학과 (박사)

현 재 서울시립대학교 컴퓨터과학부 부교수

관심분야 : 컴퓨터 보안, 영상통신, 게임기술