Scalable Fingerprinting Scheme using Statistically Secure Anti-Collusion Code for Large Scale Contents Distribution

Jae-Min Seol and Seong-Whan Kim

Department of Computer Science,
University of Seoul, Jeon-Nong-Dong, Seoul, Korea.
{seoleda@hotmail.com, swkim7@uos.ac.kr}

Abstract. Fingerprinting schemes use digital watermarks 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. Previous fingerprint code design including ACC (anti-collusion code) cannot support large number of users, which is a common situation in ubiquitous contents distribution environment. We propose a practical scalability solution, which extends previous ACC codebook generation scheme. We design a scalable ACC scheme using a Gaussian distributed random variable to increase the robustness over average and median attack. We implemented our scheme using human visual system based watermarking scheme, and the fingerprinted copy of standard test images show good perceptual quality. The result shows good collusion detection performance over average and median collusion attacks for large scale user population.

Keywords: Scalable, anti-collusion code, digital fingerprinting

1 Introduction

A digital watermark or 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. An early work on designing collusion-resistant binary fingerprint codes for generic data was based on marking assumption, which states that undetectable marks cannot be arbitrarily changed without rendering the object useless. However, multimedia data have very different characteristics from generic data, and we can embed different marks or fingerprints in overall images, which biased strict marking assumption. Recently, an improvement was to merge the low level code (primitive code) with the direct sequence spread spectrum embedding for multimedia and extend the marking assumption to allow for random jamming [1]. Min Wu 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.

We present a scalable ACC fingerprinting design scheme, which extends ACC for large number of user support. Simply replicating ACC codebook does not work, because there are ambiguous cases for determining who colluders are. We extend the ACC (anti-collusion code) scheme using a Gaussian distributed random variable for medium attack robustness. We evaluate our scheme with standard test images, and show good collusion detection performance over two powerful attacks: average and median collusion attacks.

2. Related Works

An early work on designing collusion-resistant binary fingerprint codes was presented by Boneh and Shaw in 1995 [3], which primarily considered the problem of fingerprinting generic data that satisfy an underlying principle referred to as the marking assumption. 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 design totally 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.

Fingerprint codes (e.g. c-secure codes) for generic data was intended for objects that satisfy the marking assumption, multimedia data have very different characteristics from generic data, and a few fundamental aspects of the marking assumption may not always hold when fingerprinting multimedia data. For example, different marks or fingerprints can be embedded in overall images through spread spectrum techniques, thereby it makes impossible for attackers to manipulate individual marks at will. As shown in Equation (1), Min Wu presented the design of collusion-resistant fingerprints using code modulation [2]. The fingerprint signal wj for the j-th user is constructed using a linear combination of a total of v orthogonal basis signals $\{\mathbf{u_i}\}$, multiplied by the coefficients $\{b_{ij}\}$, representing the fingerprint codes from $\{\pm 1\}$.

$$w_j = \sum_{i=1}^{v} b_{ij}\mathbf{u}_i. \qquad (1)$$

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. It has been shown that binary-valued ACC can be constructed using balanced incomplete block design

(BIBD) [4]. The definition of (v, k, λ) BIBD code is a set of k-element subsets (blocks) of a v-element set χ, such that each pair of elements of χ occur together in exactly λ blocks. The (v, k, λ) BIBD has a total of n = (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.

3. Scalable and Robust Fingerprint Scheme

Min Wu's fingerprinting scheme cannot easily extend to support large number of users because it is based on (v, k, λ) BIBD code design. Because we should have more overhead for bigger BIBD code, we designed a scalable fingerprint scheme, which can make large number of fingerprints from small BIBD code.

3.1 Codebook Design

In our scheme, we construct each user's fingerprint as the composition of ACC (w_i) and a Gaussian distributed random signal λ as shown in Figure 1. The dimension of code vectors (M) can be increased to fit the size of fingerprinting users.

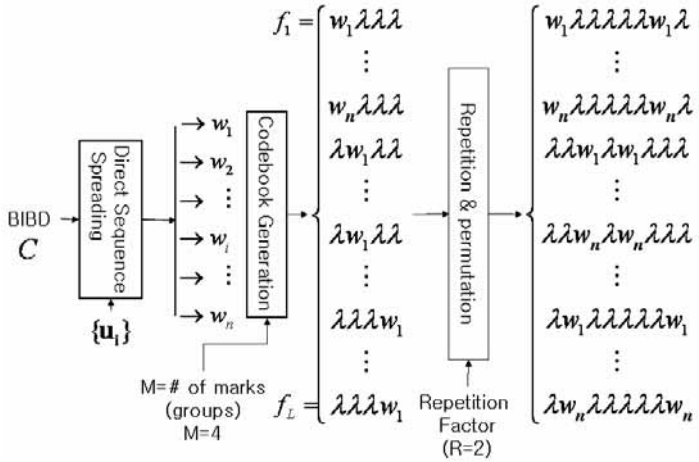


Fig. 1. Scalable fingerprint codebook, extending ACC base code with λ

We can view our scheme as a two level spreading: direct sequence spreading and frequency hopping. We used same spreading (direct sequence spreading) as ACC and

we spread the ACC over M image blocks (frequency hopped), thereby we can increase the number of fingerprint codes. This scheme has strong advantages that we can control the number of fingerprint codes easily.

3.2 Fingerprint Embedding and Detection

Once we generated the code vectors, we embed the fingerprint codes over M x R selected regions as shown in Figure 2. Fingerprinting regions (blocks) are chosen based on the model of NVF (Noise Visibility Function) [5]. Each user l's fingerprint f_l is constructed by repetition and permutation like Dan Boneh's fingerprinting scheme. For example, $w_1\lambda\lambda\lambda$ (M = 4 case) is enlarged 2 (R = 2 case) times ($w_1w_1\lambda\lambda\lambda\lambda\lambda\lambda$) and shuffled ($w_1\lambda\lambda\lambda\lambda\lambda w_1\lambda$). The permutation sequence is unique to all users, but unknown to attackers. Repetition and permutation prevent interleaving collusion attack. $f_l(i)$ is inserted signal into i-th block, each $f_l(i)$ can be ACC or λ signal, and is embedded in the M×R selected image blocks (there are R ACC signals and (M-1)× R λ signals.

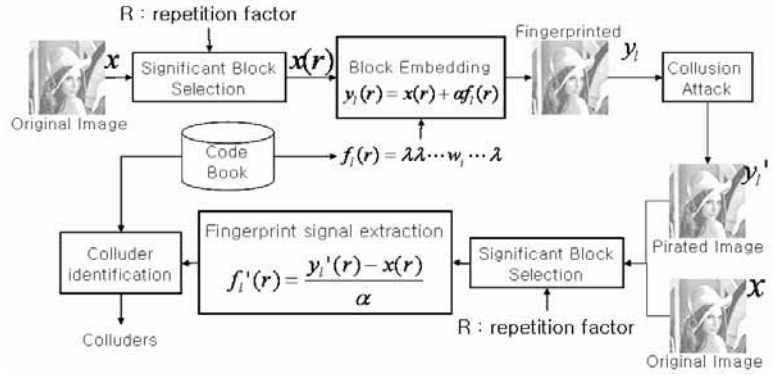


Fig. 2. Scalable fingerprint embedding / extraction of fingerprint f_l for user l

To embed ACC (w_i) signal in a specified block y_i, we use the following Equation (2). To increase the fingerprint robustness, we inserted ACC signal over R image blocks. All the ACC (w_i) are the same, however, the resulting watermark will be different, depending on $1-NVF$, which considers the local HVS masking characteristics [6].

$$y_i = x + (1-NVF)w_i, \qquad w_i = \sum_{j=1}^{v} c_{ij}\mathbf{u}_i. \tag{2}$$

$$NVF(i,j) = \frac{1}{1+\sigma_x^2(i,j)}$$

Likewise, λ signal embedding uses the following Equation (3). To un-correlate the λ signal, we use the random variable for λ signal, instead of simply choosing zero vectors. σ is used to increase median attack robustness. If we increase σ, we can increase the median attack robustness because there is little difference between λ signals and w_i; however, we can risk the decrease of detection precision.

$$y_i = x + (1-NVF)\lambda, \quad \lambda \sim N(0,\sigma^2) \tag{3}$$

We used non-blind scheme for fingerprint detection. To detect collusion, we used the collusion detection vector T, which can be computed using the same Equation (4) as Min Wu's as follows [2].

$$T_{mark\ i} = \{t_1, t_2, \cdots, t_v\} \quad = \frac{1}{R}\sum_{r=1+R\times(i-1)}^{R} \frac{f_l'(r)\cdot\{u_1,u_2,\cdots,u_v\}}{\sqrt{|f_l'(r)|^2 \times |u_i|^2}} \tag{4}$$

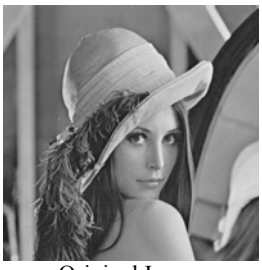
Next, $T_{mark\,i}$ vectors are converted to binary values using predefined adaptive thresholds which are determined by the mean of t_i ($\bar{t} = \frac{1}{v}\sum_{i=1}^{v} t_i$). Checking binary vector over C, if the j-th code vector ($c_{.i}$) is equal to binary values, j-th user is suspected to be traitor.

4. Analysis and Experimental Results

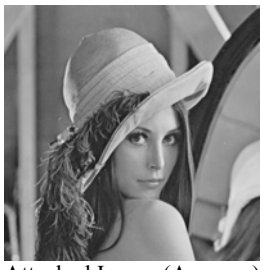
We experimented with the standard test images. Figure 3 shows test images and their enlarged fingerprints. After fingerprint embedding, the average PSNR is over 41 dB with good subjective quality.

Fig. 3. Fingerprinted images, and their fingerprints (Enlarged), the number of Marks (M) =10, Repetition factor (R) =16, Block size = 32x32: (top) Baboon (PSNR: 40.69 dB), (second) Lena (PSNR: 44.07 dB), (third) Boat (PSNR: 45.45 dB), (bottom) Barbara (PSNR: 42.72 dB)

We tested our scalable fingerprinting code for various collusion attacks (average, median, min, max, min-max, modified negative, randomized negatives) for the test images. Average collusion is widely used collusion attack [8], because it is efficient to attack fingerprints, and also it makes better image quality after collusion (usually it increases 4-5 dB). Figure 4 shows a collusion example, when six colluders make pirated copies from their fingerprinted copies. Figure 4 shows original images, and the colluded (average, median collusion) copies.



Original Image



Attacked Image (Average)
PSNR: 51.74 dB

Attacked Image (Median)
PSNR: 50.67dB

Fig. 4. Original, average, and median attacked images

We used N (0, 16) for λ signal, and we chose σ^2 as 16.0 experimentally to tradeoff between median attack robustness and false positive error rate. We can compute the probability of false positive (there is no collusion, but the λ signal makes similar results as collusion occurs) error as Equation (5). If any marks are purely linear combination of λ, their $\bar{t}$ (the mean of t_i) will be zero. Using Equation (5), we can correctly differentiate linear combination of λ and others. We use the student's T test for the mean of one normal sample [9]. For example, if $w_1\lambda\lambda\lambda$ and $\lambda w_3\lambda\lambda$ collude using average attack, we can extract signals $(w_1+\lambda)/2$, $(\lambda+w_3)/2$, $(\lambda+\lambda)/2$ and $(\lambda+\lambda)/2$ at each mark, and we can distinguish mark 1,2 and mark 3,4 using Equation (5).

$$P(\tau|H_0)=G(\tau),\ \ where\ \tau=\frac{\bar{t}-0}{S/\sqrt{v}},\ \ \bar{t}=\frac{1}{v}\sum_{i=1}^{v}t_i,\ \ S=\frac{1}{v-1}\sum_{i=1}^{v}(t_i-\bar{t})^2 \qquad (5)$$

$$G(\tau)=\int_{\tau}^{\infty}\frac{\Gamma([r+1/2])}{\sqrt{\pi r}\Gamma(r/2)}(1+w^2/r)^{-(r+1)/2}dw,\ \text{where}\ \ r=v\text{-}1$$

To increase both the detection precision and median attack robustness, we can increase the R in embedding step. If we use the average of signal over R blocks, we can correctly differentiate the linear combination of λ and others with high probability, because the variance of τ gets smaller (σ^2/R) than the variance of original signal (σ^2). Figure 5 and Figure 6 show the fingerprint detection result (T vectors) after average and median collusion attacks with detection threshold mean of t_i set. (Because as colluders are increase, the amplitude of t_i are decreased) We used the same detection procedure as average collusion attack, and show the same colluder identification. Median attack is a powerful attack; however, our approach shows good performance. Setting the significant level of H_0 to 0.05, we will suspect the users in mark 1, 3, and 7.

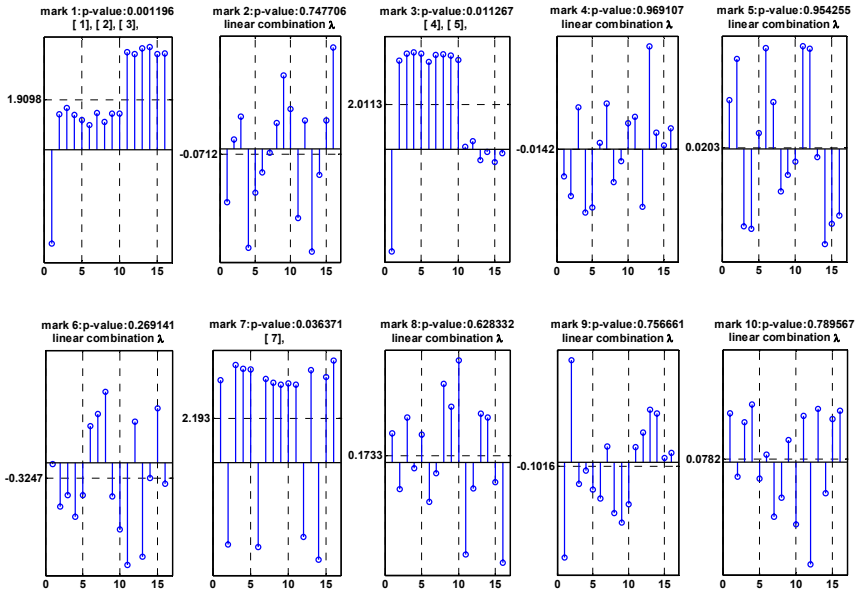


Fig. 5. Detection result after average attack

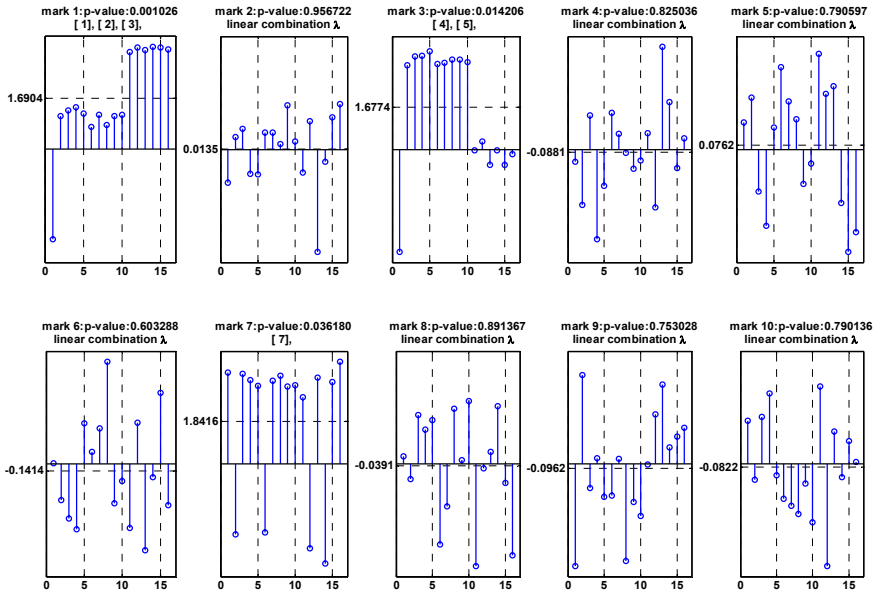


Fig.6. Detection result after median attack

Decoding mark 1, mark 3and mark 7, we can compute T vectors {0000 0000 0011 1111}, {0111 1111 1100 0000}.and {1011 10111 110 1011}, as shown in Figure 5 and Figure 6. Checking T vectors over (16, 4, 1) BIBD code matrix as shown in

Figure 7, we can suspect $\{w_1, w_2, w_3\}$ in mark 1 $\{w_4, w_5\}$ in mark 3 and $\{w_7\}$ in mark 7 as colluders. Using codebook design rule, we can know that colluders are users with fingerprint code C = $\{w_1\lambda\lambda\lambda\lambda\lambda\lambda\lambda\lambda\lambda, w_2\lambda\lambda\lambda\lambda\lambda\lambda\lambda\lambda\lambda, w_3\lambda\lambda\lambda\lambda\lambda\lambda\lambda\lambda\lambda, \lambda\lambda w_4\lambda\lambda\lambda\lambda\lambda\lambda\lambda, \lambda\lambda w_5\lambda\lambda\lambda\lambda\lambda\lambda\lambda, \lambda\lambda\lambda\lambda\lambda\lambda w_7\lambda\lambda\lambda\}$

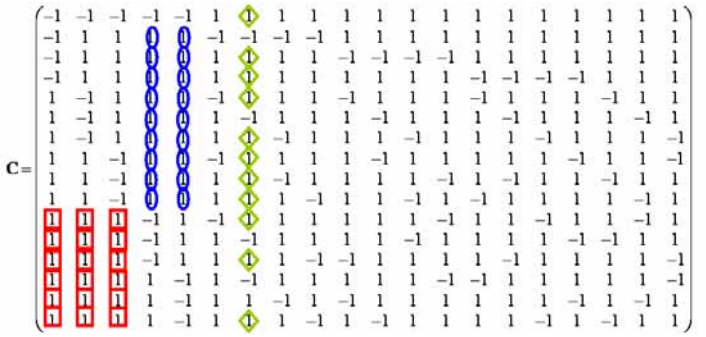


Fig. 7 Matching marks in (16, 4, 1)-BIBD code matrix for colluder detection

We analyzed the average number of fingerprinted images to erase fingerprints (successful collusion). Figure 8 shows that colluders should have 40 fingerprinted images (or 40 colluding members) on average case, to erase the fingerprints for our scalable fingerprinting scheme with (16, 4, 1) BIBD and scalability m = 40. If we use the larger BIBID codes (e.g. (61, 5, 1) BIBD code), we can get much bigger collusion robustness.

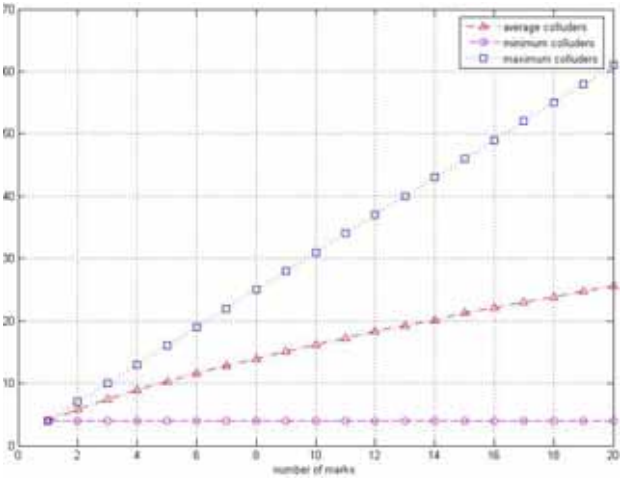


Fig.8. Number of marks (m) versus average number of colluder for successful collusion

5. Conclusions

In this paper, we presented a scalable ACC fingerprinting scheme, which covers large number of fingerprint codes. Previous fingerprint code design including ACC (anti-collusion code) cannot support large number of users. 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.

References

1. Yacobi, Y.: Improved Boneh-Shaw content fingerprinting. in Proc. CTRSA2001 (2001) 378–91
2. Trappe, W., Wu, M., Wangm Z. J., Liu, K. J. R.,: Anti-collusion fingerprinting for multimedia. IEEE Trans. Signal Proc. vol. 51, Apr. (2003) 1069-1087
3. Boneh, D., Shaw, J.: Collusion-secure fingerprinting for digital data. IEEE Trans. Inform. Theory, vol. 44, Sept. (1998) 1897–1905
4. Colbourn, C. J., Dinitz, J. H.: The CRC Handbook of Combinatorial Design. Boca Raton, FL: CRC Press (1996)
5. Voloshynovskiy, S., Herrige, A., Baumgaertner, N., Pun, T.: A stochastic approach to content adaptive digital image watermarking. Lecture Notes in Computer Science: 3rd Int. Workshop on Information Hiding, vol. 1768, Sept. (1999) 211-236
6. Watson, A. B., Borthwick, R., Taylor, M.: Image quality and Conf. Human Vision, Visual Processing, and Digital Display VI (1997)
7. 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)
8. Zhao, H., Wu, M., Wang, J., Ray Liu, K. J.: Nonlinear collusion attacks on independent Fingerprints for multimedia. ICASSP. vol. 5, Apr. (2003) 664-667
9. V. K. Rohatgi, “An Introduction to Probability Theory and Mathematical Statistics”, John Wiley & Sons, Inc. (1976)