World Academy of Science, Engineering and Technology
International Journal of Electrical and Computer Engineering
Vol:1, No:2, 2007

Hybrid Modulation Technique for Fingerprinting

Hae-Yeoun Lee, In-Koo Kang, and Heung-Kyu Lee

***Abstract*—**This paper addresses an efficient technique to embed and detect digital fingerprint code. Orthogonal modulation method is a straightforward and widely used approach for digital fingerprinting but shows several limitations in computational cost and signal efficiency. Coded modulation method can solve these limitations in theory. However it is difficult to perform well in practice if host signals are not available during tracing colluders, other kinds of attacks are applied, and the size of fingerprint code becomes large. In this paper, we propose a hybrid modulation method, in which the merits of orthogonal modulation and coded modulation method are combined so that we can achieve low computational cost and high signal efficiency. To analyze the performance, we design a new fingerprint code based on GD-PBIBD theory and modulate this code into images by our method using spread-spectrum watermarking on frequency domain. The results show that the proposed method can efficiently handle large fingerprint code and trace colluders against averaging attacks.

***Keywords*—**Fingerprinting, GD-PBIBD theory, Hybrid modulation technique.

I. Introduction

Digital fingerprinting is a kind of copyright protection technique that traces the illegal distribution of copyrighted contents. A unique fingerprint code that identifies a recipient is embedded into host contents for selling or distributing. When copies of the content are found from illegal route, the content seller can identify traitors who had distributed the content illegally by detecting the embedded fingerprint code.

Averaging attack is a serious problem in digital fingerprinting. Since digital fingerprinting technique embeds slightly different codes according to the customers, several fingerprinted contents, but based on identical contents are available to attackers. The averaging attack is an attempt to remove the embedded fingerprints by using several copies of the content. For example, adversaries can estimate the original content without fingerprints by averaging several fingerprinted copies.

Orthogonal modulation approach is a straightforward method and widely used for digital fingerprinting. However, it shows several limitations in computational costs, signal (or code) efficiency, and robustness against averaging attacks. Another approach to solve these limitations is using collusion-resistant fingerprint codes, so called as coded modulation method, that are not affected by averaging attacks. Boneh presented a code system named "Frame-proof code" and that satisfied for preventing the false detection of a recipient who did not join in averaging attacks [1]. Stinson first proposed a fingerprint code system that satisfied frame-proof property by using a combinatorial design theory [2]. Trappe presented a fingerprinting method for images by using BIBD (Balanced Incomplete Block Design) theory [3]. Section II will explain how these modulation methods work, how colluders are traced, and what their problems are in detail.

In this paper, to solve problems from orthogonal modulation method and coded modulation method, we propose a new hybrid modulation method, in which the merits of orthogonal modulation method and coded modulation method are combined so that we should achieve low computational cost, high signal efficiency and robustness against averaging attacks. We also design a new fingerprint code based on GD-PBIBD (Group Divisible Partially Balanced Incomplete Block Design) theory. GD-PBIBD is one of combinatorial design theories and can flexibly control elements replication numbers in blocks such that the resulting fingerprint code has high efficiency than BIBD. For experiments, we use spread-spectrum watermarking on frequency domain to embed and detect fingerprints of each user and the results show that the proposed modulation method could efficiently trace colluders against averaging attacks.

In following sections, we will describe orthogonal modulation technique and coded modulation technique. Then, our hybrid modulation method will be explained. The performance will be analyzed and discussed in section IV.

II. Previous Fingerprinting Schemes

A. Orthogonal modulation method

Orthogonal modulation approach is a straightforward method for digital fingerprinting. In this method, N orthogonal signals are used to accommodate N users, i.e. each user has their own orthogonal signal and this orthogonal signal is inserted into host signals, called as contents, by digital watermarking techniques. To decide which user owns contents or joins to make illegal copies, N correlations are computed such that computation complexity is related to the number of users. By designing tree-structured detection strategy for orthogonal modulated fingerprinting, complexity can be partly solved [3].

An additional drawback is that when the number of users increases, the strength of orthogonal signals inserted into host signals will be attenuated and the colluders cannot be clearly detected. Assume that correlation is used as detection statistics and M users join to make illegal copy C_j.

Hae-Yeoun Lee is with Department of EECS, Korea Advanced Institute of Science and Technology, Republic of Korea, (corresponding author to provide phone: +82-42-869-5566; email address: hytoiy@casaturn.kaist.ac.kr)

In-Koo Kang and Heung-Kyu Lee are also with Department of EECS, Korea Advanced Institute of Science and Technology, Republic of Korea (email address: { ikkang | hklee }@casaturn.kaist.ac.kr)

$$Corr = \frac{1}{N}\sum S_i C_j \quad \text{where } C_j = \frac{1}{M}\sum_M S_k \tag{1}$$

The signal of each user is orthogonal so that correlation will be decreased inverse-proportional to the number of colluders *M* as follows.

$$Corr = \frac{1}{MN}\sum S_i S_j \tag{2}$$

Assume that normalized correlation is used as detection statistics. Each signal is orthogonal and follows a gaussian distribution model so that the norm of vector C_j is represented as follows.

$$N.C. = \frac{\sum S_i C_j}{\| S_i \| \cdot \| C_j \|} \quad \text{where } \| C_j \| = \frac{1}{\sqrt{M}} \| S_i \| \tag{3}$$

Normalized correlation is inverse-proportional to the square root of the number of colluders *M* as follows.

$$N.C. = \frac{1}{\sqrt{M}} \frac{\sum S_i S_j}{\| S_i \| \cdot \| S_j \|} \tag{4}$$

Theoretical analysis shows the limit of detector when orthogonal signals are averaged and we can find that when the large number of users joins to make illegal copies, orthogonal modulation scheme will fail to retrieve colluders successfully.

B. Coded modulation method

Coded modulation method is used to accommodate more users than orthogonal modulation method with the same amount of orthogonal signals. Furthermore, high robustness against averaging attacks is achieved by using collusion secure codes.

Trappe proposed a representative coded modulation method based on fingerprinting code designed by BIBD theory [2]. That is anti-collusion codes and the composition of any subset from code vectors is unique, which allows identifying colluders.

A watermark signal for one user is acquired by modulating with codes and orthogonal signals as follows.

$$w_j = \sum_{i=1}^{M} b_{ij} u_i \tag{5}$$

where b_{ij} is a code vector of user *j* and u_i are basic orthogonal signals. After the watermark signal is inserted into host signals, each b_{ij} can be determined by calculating correlation with u_i and comparing against a threshold.

If a sequence of fingerprint code has been averaged, the detected sequence will be the logical AND-ed operation of the fingerprint code. By comparing the bit position of resulting sequence whose value is 1 in fingerprint code, we can find out which user is involved in coalition out of innocent users. Assume that two users collude and their code vectors are (0111) and (1110) respectively, then the detector will output a (0110) code vector. Through matching the bit position of 1 from the (0110) code vector, colluders can be traced.

Problem of their scheme is that it is impossible or difficult to select threshold values to determine resulting code vectors in practice. For example, 7 users join to make illegal copies and their code vector is (0, 1, …) for one user and (1, 1, …) for other users. In order to trace colluders correctly, the resulting code (0, 1, …) must be detected. In ideal non-blind strategy without attacks except averaging, when we use linear correlation as detection statistics, the correlation value from the second item will be higher than that from the first one because the second item of each user is all 1 so that the strength of basis orthogonal signals will be reserved in collusions, but the first item of each user is different so that the strength of basis orthogonal signals will be decreased in proportion to | # of 1 - # of 0 | / | # of colluders |. When normalized correlation, generally used for detector because their output is refined from –1.0 to 1.0 and decision boundary can be selected easily, is used as detection statistics, correlation values from two items will be almost equal to 1.0 and that will make difficult to find the colluded fingerprint code correctly. In blind strategies and other kind of attacks, it will become worse. Exact extraction of basis orthogonal signals is impossible without original host signals and basic orthogonal signals can be distorted by simple attacks. Therefore, there are many situations that correlation from the first item can be greater than that from the second item. When the size of fingerprint code becomes larger, it will be more problematic.

III. Hybrid Modulation Technique

As explained before, coded modulation technique described by Trappe shows severe problems during the detection of the colluded fingerprint code. In this section, we propose a hybrid modulation technique to embed and detect fingerprint code. This technique can handle the large size of fingerprint code with efficiency. We will first describe a new fingerprint code from GD-PBIBD theory and then explain a hybrid modulation technique

A. Fingerprinting code based on GD-PBIBD design

Similarly to coded modulation method, it is important to design an efficient fingerprint code for our hybrid modulation method. We tried to find out design theories for a new efficient fingerprint code focusing on high code efficiency as well as averaging resiliency. Code efficiency refers to the number of recipients that can be handled by designed code length. In [3], a fingerprint code based on (16,20,5,4,1) BIBD theory admits 20 users by using 16 bits code so that their code efficiency is 1.25. The higher code efficiency means the effectiveness of fingerprinting system and the better content fidelity and robustness can be achieved by using less bits of information for the same performance.

We found that GD-PBIBD theory would be resilient against averaging attacks and present high code efficiency ratio. $(v, b, r, k, \lambda_1, \lambda_2)$ GD-PBIBD is one of combinatorial design and that divides *v* elements into *b* blocks [4] [5]. In order to create blocks, GD-PBIBD theory classifies *v* elements into two groups according to group divisible association scheme in intermediate stage such that any two elements are in the same group λ_1 times and the different groups λ_2 times.

Differently from BIBD theory in which there is only one group and any two elements present only λ_1 times, we can

	S1	S2	S3	…													S16	S17	S18
User1:	0000	0000	1111	1111	1111	1111	1111	1111	1111	1111	1111	1111	1111	1111	1111	1111	1111	1111	1111
User2:	1111	1111	1111	1101	1111	0111	1110	1111	1111	1111	0111	1011	1011	1111	1101	1111	1111	1111	1110
User3:	1111	1111	1111	1110	1111	1011	1111	0111	1011	1111	1111	1101	0101	1111	1110	1111	1111	1111	1111
User4:	1111	1111	1111	1111	1111	1101	1111	1011	1101	1111	1111	1110	1110	1111	0111	0111	1011	1111	
User5:	1111	1111	1011	1111	1111	1111	0111	1110	1111	1111	1111	1111	1111	1011	1111	1101	1010	1111	
User6:	1111	1111	0101	1111	1111	1111	1111	1110	1111	0111	1011	1111	1111	1011	1111	1101	1110	1111	
User7:	1111	1111	1110	1111	0011	1111	1111	1111	1111	1011	1101	1111	1111	1101	1111	1110	1111	0111	
User8:	1111	1111	1111	0111	1101	1111	0011	1111	1111	1101	1110	1111	1111	1110	1111	1111	1111	1111	
…																			

Figure 1. Part of 72×89 fingerprint code based on GD-PBIBD design (S*no* represent segment #).

flexibly control the number of element presence in blocks using GD-PBIBD theory and make more blocks than BIBD theory. GD-PBIBD also has averaging resiliency up to *k-1* blocks that is equal to BIBD. Fig. 1 shows parts of a fingerprint code designed by (72,89,9,8,0,1) GD-PBIBD theory that can accommodate 89 users with 72 bits code and trace maximum 7 colluders. Code efficiency will be 1.24. In case of BIBD theory to trace maximum 7 colluders, 64 bits code accommodating 72 users is required so that code efficiency will be 1.12.

B. Embedding technique

For the convenience of our explanation, we will describe the proposed modulation method using (72,89,9,8,0,1) GD-PBIBD theory.

The way to embed an *M* bits length fingerprint code into host signals is described as follows.

1) Split an *M* bits length fingerprint code into segments by grouping *N* bits unit.
2) Embed an *N* bits grouped code for each segment by using orthogonal modulation method.

In coded modulation method, *M* orthogonal signals must be considered for an *M* bits length fingerprint code. However, for the efficiency, we divided an *M* bits length fingerprint vector into several segments by grouping *N* bits. For each segment, one orthogonal signal based on an *N* bits code is generated and embedded by using orthogonal modulation method. In this case, there are *M/N* segments so that only *M/N* signals are used for orthogonal modulation method. For example, in (72,89,9,8,0,1) GD-PBIBD design, we split a 72 bits length fingerprint code into 18 segments by grouping 4 bits such that we only have to embed 18 signals not 72 signals.

When the number of grouping bits *N* becomes higher, we can increase the efficiency of embedding. However, maximum 2^N signals can be used to collude and that is related to the maximum of correlation. Theoretical analysis described in section II will be helpful to determine the number of grouping bits.

In our experiments using GD-PBIBD theory, we group by 4 bits unit and use normalized correlation as detection statistics so that there can be maximum 16 cases. When all cases are used for averaging attacks, theoretical correlation will be 0.25. Fortunately, in each segment, GD-PBIBD has maximum 10 cases so that theoretical correlation becomes 0.32 and it will be helpful to increase robustness in detection stage.

C. Detection technique

The way to trace colluders is as follows.

1) For each segment
   A. Detect all orthogonal signals embedded by using orthogonal modulation method
   B. Determine *N* bits code of retrieved orthogonal signals and apply logical AND operation of all *N* bits code
2) Construct an *M* bits length code by concatenating the result codes from all segments.
3) Detect colluders by comparing the *M* bits code with fingerprint code.

In detection phase, we can determine the embedded *N* bits code of each segment by extracting the embedded orthogonal signals by using correlation-based detector. If collusion attacks have been applied, several orthogonal signals may be extracted from one segment. In this case, we first construct the bits code for each extracted orthogonal signal, and make a colluded bits code by applying logical bits AND operation with the constructed bits codes. The logical AND-ed bits code for all segments then are concatenated. Using this concatenated code, we can find out the colluders through inspecting the fingerprint code by applying the colluder finding method similar to coded modulation method. For example, when we insert an orthogonal signal representing (1111), a 4 bits grouped code, into a segment during embedding stage, it can be easily retrieved by orthogonal modulation method in detection stage. If three segments where orthogonal signals representing (1111), (1010), and (0011) respectively are colluded by averaging attacks, we can detect three signals representing (1111), (1010), and (0011) and hence acquire the resulting code (0010) by applying logical bits AND operation. The concatenated code from each segment is used for tracing colluders.

Similar to the method of [3], our proposed method also requires selecting threshold values used to determine whether an orthogonal signal exists or not. However, we can easily select thresholds by analyzing the false error probability of detector in orthogonal modulation method.

IV. Performance Analysis and Discussions

We carried out experiments to analyze the performance of our hybrid modulation method by using the fingerprint code constructed by (72,89,9,8,0,1) GD-PBIBD theory. This code can accommodate 89 users, the length of a code vector for one user is 72 bits, and maximum 7 collusions can be traceable.

6 CIF format sized (352×288) images are used as host signals and non-blind watermarking strategy using discrete cosine transform is applied to embed / detect orthogonal signals into / from host signals. For imperceptibility, an orthogonal signal is inserted into the middle frequency of discrete cosine transform and normalized correlation is used as detection statistics. The

error probability of normalized correlation based detector follows a gaussian distribution model [6]. By using 100 random orthogonal signals and 100 random images, we analyzed detection statistics and selected the reliability of detector as 10^{-4} by using threshold value as 0.124.

As mentioned previously, we split a 72 bits length fingerprint code into 18 segments by grouping 4 bits unit. In each segment, there are maximum 10 cases. In theoretical analysis, the output of normalized correlation based detector will be 0.32 and this value is higher than threshold values to determine the resulting code from each segment such that our modulation method will be efficiently trace colluders.

To insert 18 orthogonal signals into host signals, we divide images into 18 blocks as shown in Fig. 2 whose size is 64×64 pixels and a 1024 length orthogonal signal representing a 4 bits code from one segment is inserted into each block. PSNR of images after fingerprinting is over 43db and imperceptible to native eyes. A residual image between the original image and the fingerprinted image is shown in Fig. 3.

Figure 2. 18 segmented blocks of a CIF image.

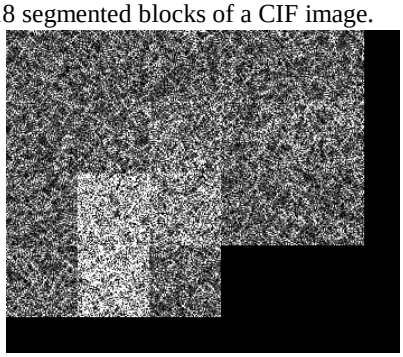

Figure 3. Residual image.

For each image, we have generated 100 illegal images by colluding 1 user, 2 users, 3 users, 4 users, 5 users, 6 users, and 7 users respectively and tried to trace colluders.

For each colluding case, table I summarizes colluder detection results from 100 illegal copies of 6 images. In most of experiments, because we applied non-blind strategy, we can trace colluders successfully and colluded orthogonal signals could be retrieved accurately except 7 colluding cases. However, when 7 users colluded, the performance was decreased because the applied watermarking scheme attenuated the embedding strength of the orthogonal signal for imperceptibility so that the embedded signals were severely removed by colluding in some parts of images.

In this paper, we have performed experiments by using non-blind watermarking strategy and only averaging attacks. Our on-going research is advancing our hybrid modulation method by using blind watermarking strategy and applying various attacks such as spatial filtering, JPEG compression, and so on. In our opinions, the embedded orthogonal signals cannot be retrieved exactly so that the performance will be decreased. However, we expect that our modulation algorithm will work better than orthogonal modulation or coded modulation method alone.

TABLE I. DETECTION RESULTS FROM 100 ILLEGAL COPIES OF 6 IMAGES FOR EACH COLLUDING CASE.

	Number of extracted colluders						
	1	2	3	4	5	6	7
1 colluder	600	-	-	-	-	-	-
2 colluders	-	600	-	-	-	-	-
3 colluders	-	-	600	-	-	-	-
4 colluders	-	-	-	600	-	-	-
5 colluders	-	-	-	-	600	-	-
6 colluders	-	-	-	-	-	600	-
7 colluders	-	-	-	-	1	75	524

V. CONCLUSIONS

Generally, considering fingerprint code can increase signal efficiency and resiliency to averaging attacks. However, in order to accommodate many users, the large size of fingerprint code must be considered such that effective modulation technique will be essential. We first described a new fingerprint code based on GD-PBIBD theory that would have more signal efficiency comparing to that of BIBD theory. We then proposed a hybrid modulation technique that could handle the large size of fingerprint code. We conducted practical experiments on several images and the results showed considerable performance on extracting colluded fingerprint code and tracing colluders precisely under averaging attacks. We convinced that the proposed hybrid modulation method could provide a solution of the problems caused by handling the large size of fingerprint code and averaging attacks.

REFERENCES

[1] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. On Information Theory*, vol. 44, 1998, pp. 1897-1905.
[2] D. R. Stinson and R. Wei, "Combinatorial properties and constructions of traceability schemes and frameproof codes," *Journal of Discrete mathematics*, 1997.
[3] W. Trappe, M. Wu, Zhen Wang, and K.J.R. Liu, "Anti-collusion Fingerprinting for Multimedia," *IEEE Trans. On Signal Processing*, vol. 51, 2003, pp. 1069-1087.
[4] C. J. Colbourn and J. H. Dinitz, The CRC Handbook of Combinatorial Designs, CRC, 1996.
[5] Willard H. Clatworthy, Tables of two-associate-class partially balanced designs, National Bureau of Standards Washington, D.C., U.S., 1973.
[6] I. J. Cox, M.L. Miller, and J.A. Broom, Digital Watermarking, Morgan Kaufmann Publishers: San Francisco, CA, 2002, Chapter 5.
[7] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT domain system for robust image watermarking," *Signal Processing*, vol. 66, 1998, pp. 357-372.