A New Fingerprint Design Using Optical Orthogonal Codes

by

Na Zhao

A Thesis

Presented to Lakehead University

in Partial Fulfillment of the Requirement for the Degree of

Master of Science

in

Electrical and Computer Engineering

Thunder Bay, Ontario, Canada

April 22, 2014

UMI Number: 1562568

All rights reserved

INFORMATION TO ALL USERS
The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript
and there are missing pages, these will be noted. Also, if material had to be removed,
a note will indicate the deletion.

UMI 1562568

Published by ProQuest LLC (2014). Copyright in the Dissertation held by the Author.

Microform Edition © ProQuest LLC.
All rights reserved. This work is protected against
unauthorized copying under Title 17, United States Code

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

Abstract

Na Zhao. A New Fingerprint Design Using Optical Orthogonal Codes .

Digital fingerprinting has been proposed to restrict illegal distribution of digital media, where every piece of media has a unique fingerprint as an identifying feature that can be traceable. However, fingerprint systems are vulnerable when multiple users form collusion by combining their copies to create a forged copy. The collusion is modeled as an average linear attack, where multiple weighted copies are averaged and the Gaussian noise is then added to the averaged copy. In this thesis, a new fingerprint design with robustness to collusion is proposed, which is to accommodate more users and parameters than other existing fingerprint designs. A base matrix is constructed by cyclic shifts of binary sequences in an optical orthogonal code and then extended by a Hadamard matrix. Finally, each column of the resulting matrix is used as a fingerprint. The focused detection is used to determine whether a user is innocent or guilty in average linear attacks. Simulation results show that the performance of our new fingerprint design is comparable to that of orthogonal and simplex fingerprints.

Contents

List of Figures

List of Tables

List of Symbols

F – Fingerprint System.
Z_L – Load impedance.

List of Abbreviations

OOC – Optical Orthogonal Codes.
FHT – Fast Hadamard Transform.
ETF – Equiangular Tight Frames.
WNR – Watermark Noise Ratio.

Chapter 1

Introduction

1.1 Digital Fingerprint Techniques

We have been through the period of transition between industrial society and information society with revolution of information technology. Digital information products have a more important impact on our life than ever before. Smart phone, digital camera, MP3 player and other digital products become inseparable in our daily life through which we can enjoy music, photos and videos. Moreover, internet provides a platform and thus we can share digital multimedia with others. On one hand, the internet technology inspires us to enjoy and deliver multimedia in a broader range. On the other hand, it also facilitates unauthorized distribution and illegal alteration.

Illegal distribution has adverse effects on commercial applications, which results in harming the interests of publishers. More seriously, disclosure of confidential files has immeasurable consequences on institutions and organizations. Take music industry as an example, the International Federation of Phonographic Industry (IFPI) reports that global music piracy is still a big concern. It estimates that 37% of all CD purchases are pirate copies, and puts their value at $4.5 billion. It also estimates that 20 billion songs were downloaded for free worldwide. Copyright protection is crucial to safeguard intellectual and economic resources. Access control is one fundamental approach to protect digital content, which prevents illegal distributors from accessing content. Multimedia forensics is another important method applied for copyright protection,

which detects illegal manipulation and identifies unauthorized users.

Digital fingerprint technology is one important branch of multimedia forensics for copyright protection. Its goal is to deter users from illegally distributing the digital contents ensuring that it is used for the intended purpose. Digital fingerprinting is an effective technique to make the media files uniquely identifiable. Once digital media files are illegally distributed, the content owner (or the publisher) can trace them through the unique signature. In this way, the fingerprint is a threat, which deters the users to release unauthorized copies. The fingerprints should be imperceptible to the original multimedia content and meanwhile can survive from attacks. In this way the content owner can successfully identify the attackers without sacrificing the quality of multimedia.

However, there is one problem in digital fingerprinting: multiple users can collude to identify or distort a fingerprinted copy and make the content owner difficult to detect distributors. Users with different fingerprinted copies conspire and combine their copies to remove or distort their fingerprints. These attacks are known as collusion attacks, which make improperly designed systems vulnerable since a small coalition of colluders can complete a forged copy with no detectable trace. Therefore, it is necessary for the fingerprint design to be robust to attacks.

Our research focuses on issues about collusion attacks and study to design a new fingerprint system with resistance to collusion attacks.

1.2 Literature Review

Prior works in digital fingerprinting mainly focus on studying the analysis of collusion attacks and the collusion resistance of fingerprinting systems. The analysis of collusion attacks includes the methodology of attacks, the number of colluders and types of attacks. The studies of collusion attacks facilitate to analyze the collusion resistance of fingerprint systems and design effective fingerprint systems with robustness.

1.2.1 Analysis of Collusion Attacks

[1] and [2] studied the methodologies of collusion attacks for generic data and multimedia data, respectively. For generic data, [1] proposed that colluders compared their copies to acquire the different values of certain code bits and regarded such codes as fingerprint codes. Multimedia

data has different characteristics from generic data: multimedia data has natural robustness to distortion by minoring variations of values. This characteristic of multimedia data makes the fingerprint codes too long to be removed from host data without perceptual loss while the fingerprint codes for generic data can be easily detected and changed. [2] introduced average collusion attack model for multimedia data, which was the common type of collusion attacks. The average collusion attack model is analyzed in detail in the following chapter of this thesis.

In [3], F. Ergun, **J.** Killian, and R. Kumar put that $O\sqrt{N/\log N}$ colluders were enough to attack a fingerprint system, where N is the length of signals. Similar results about the number of the maximum tolerated colluders can be found in [4] and [5]. [5] presented the parameters related to the maximum tolerated colluders of a fingerprint system. The parameters included the length of host signals, the total allowable users and the requirement of the system performance.

The author of [2] studied several types of attacks and particularly presented that nonlinear attacks were more efficient than linear attacks. The analysis of collusion attacks provided a good foundation for the design of fingerprint systems with resistance to collusions. There are two approaches in design of robust fingerprints : using *making assumption* and using *distortion assumption*.

1.2.2 Collusion Resistance of Fingerprinting System

Marking assumption

In marking assumption domain, the content owner assign a collection of marks also known as a codeword to the distributed copy. The collection of marks consists of a fingerprinting system. Previous researchers focused on shortening the length of the codeword to improve the efficiency of fingerprinting systems.Boneh and Shaw [1] first presented a fingerprint design requiring code length $O(k^4 \log k)$, which can catch at least one colluder out of k colluders with high probability. They uniquely marked and registered copies of digital data via assigning code-words. [6] proposed a similar work to [1], which investigated the leakage of decryption keys instead of detecting digital content. Compared to Boneh and Shaw's design, Tardos [7] presented a fingerprint design with a shorter length of code. H. Chu, L. Qiao, and K. Nahrstedt proposed a two-layer fingerprint system in [8], which integrated with the outer Boneh-Shaw codes. The Boneh-Shaw schemes

were also used to construct complex schemes with better anti-collusion properties in [9] and [10]. S. Lin, M. Shahmohammadi, and H. El Gamal [11] applied the minimum distance decoding scheme to identify one colluder out of all the colluders under any collusion attack that satisfied the marking assumption. There are also several works on researching the relationship between multiple access channels and fingerprint problems [12]-[14]. There are other works on developing binary fingerprint codes, including [15]-[20].

Under marking assumption, the fingerprint is used as a "mark" to label each copy. In essence, the content owner insert additional information which can be used to identify each user. Such a fingerprint has no impact on the original digital data. Different from marking assumption, in distortion assumption regime, the fingerprint is embedded into the original data, which distort the original data to some extent. In the following section, we introduce the embedding process and how to control the distortion to maintain the quality of original digital data.

distortion assumption

Another approach to design robust fingerprints uses distortion assumption. In this regime, a unique fingerprint introduces a noise-like distortion to digital media. The power of the fingerprint added by a content owner should be limited to preserve the quality of original media. The fingerprints should be perceptually invisible if the original media is image data. In terms of distortion assumption, fingerprinting technology involves embedding process, which strengthens robustness by making it hard for colluders to identify or distort fingerprints through comparisons.

Watermarking relevant to fingerprinting is well-known technology in this regime. Cox [21] proposed a secure algorithm by inserting a watermark constructed as an independent and identically distributed (i.i.d) Gaussian random vector. The insertion should guarantee the overall quality of multimedia and makes colluders difficult to remove the watermark. To achieve this goal, embedding process is necessary. Only several colluders may successfully detect or distort the fingerprints without damaging digital media if identify basis is employed as orthogonal fingerprints, where embedding process is not available. [21] was inspired by spread spectrum communications and thus rotated the basis to make the fingerprints distributed across significant dimensions of signals. In this way, it is difficult for the colluders to remove or distort the

fingerprints. More efforts of watermarking can be found in [22]-[24].

Wang *et al.* [25] proposed a specific fingerprint design using Gaussian distributed fingerprints and orthogonal modulation. They considered an averaging collusion attack to analyze robustness of the designed fingerprint system. Kiyavash *et al.* [26] proposed an optimal structure n-simplex fingerprints in term of maximizing the error exponent of the detection test. Recently, Fickus, Mixon and Tremain [27] designed a fingerprint system using equiangular tight frames (ETF), where they used the Steiner system to construct a base matrix and then extended it by a Hadamard matrix.

1.3 Motivation

The performance of Steiner ETF fingerprints is comparable to that of the orthogonal and simplex fingerprints, but they can accommodate more users. Steiner ETF fingerprints have obvious advantages over orthogonal and simplex fingerprints in term of the number of accommodated users. However, two concerns of ETF fingerprints may be raised for practical applications [34]. First, it consumes large storage since all the incidences of a Steiner system need to be stored. In practice, the fingerprint systems are applied to a large number of users and thus storage problem becomes more serious. Second, it is difficult to obtain many parameters for the length of signals and the number of accommodated users due to the limitation of optimal Steiner system [27]. To overcome these potential drawbacks, we introduce a new fingerprint system using optical orthogonal codes. Our new fingerprint system is under distortion assumption.

1.4 Thesis Contributions and Outline

In this thesis, we present a new fingerprint design using optical orthogonal codes (OOC) under distortion assumption. First, each cyclic shift of a sequence in an OOC is arranged as each column of a base matrix. Then, a Hadamard matrix is employed to extend the base matrix, and each column of the resulting matrix is used as each user's fingerprint.

The new fingerprints are similar to Steiner ETF fingerprints [28] with a more flexible structure. In Steiner ETF fingerprints, a $(2, k, v)$ Steiner system is used to construct a base matrix. All the elements of the base matrix need to be stored. We only need to remember a few binary

sequences instead of a full base matrix, which requires less storage space in practical implementation. Also, our new fingerprints can accommodate more users than some proposed fingerprints, for example, orthogonal and simplex fingerprints. Finally, we can use the fast Hadamard transform technique to improve the speed of construction and detection processes.

The thesis is organized as follows. We start with the overview of digital fingerprinting system. In Chapter 2.1 the general framework of fingerprinting system is given. Then, three typical fingerprints designs are presented in Chapter 2.2. In Chapter 2.3, we consider the performance criteria and the requirements of fingerprint systems.

In Chapter 2, we also give a general framework of digital fingerprinting techniques including fingerprints embedding, collusion attacks and detection process. The mathematical formulations are used to represent fingerprinted copies, average attacks and detector. Moreover, a brief introduction of other typical attack models is given.

In Chapter 3 and 4, we address the construction of our new fingerprint design. In Chapter 3.1 and 3.4, the fundamental definitions of optical orthogonal codes and modular Golomb ruler are presented along with their methods of construction. In Chapter 4, we present the error analysis of new fingerprint system to better comprehend its property.

In Chapter 5, fast detection process is proposed. In Chapter 6, we show the simulation results and analyze the performance of different fingerprint systems. In Chapter 7, we draw the conclusion and discuss future works.

Chapter 2

Digital Fingerprinting System

2.1 Overview of Digital Fingerprinting System

Figure 2.1 presents how the digital fingerprinting system works, which can be divided into three parts: embedding fingerprints, collusion attacks and detection process [41].

2.1.1 Embedding Fingerprints

In the first stage, i.e., embedding fingerprints, a unique fingerprint is assigned to each user. For example, a digital fingerprint $\mathbf{f}_1$ is embedded into a multimedia document $\mathbf{y}_1$, which is distributed to Alice, one of the legal users. The multimedia document could be text, audio, image, video or other digital contents. In order to protect the digital contents, the fingerprints should be robust, that is, difficult to remove from the content. If the location of the fingerprint is known, then attempts to remove or destroy the fingerprints should be detected. In this case the embedded fingerprints must meet the requirements [41]:

Imperceptibility : The fingerprinted copy of Alice $\mathbf{y}_1$ should be perceptually the same as the host signal $\mathbf{s}$.

Robustness : The fingerprint should be robust to the unintentional signal processing: cropping, rotating, attenuating, removing or other processes.

2.1.2 Collusion Attacks

In the second stage, multiple users, for example, Alice and Bob, may collude to forge a copy and illegally redistribute the document after the multimedia document is distributed to the users,

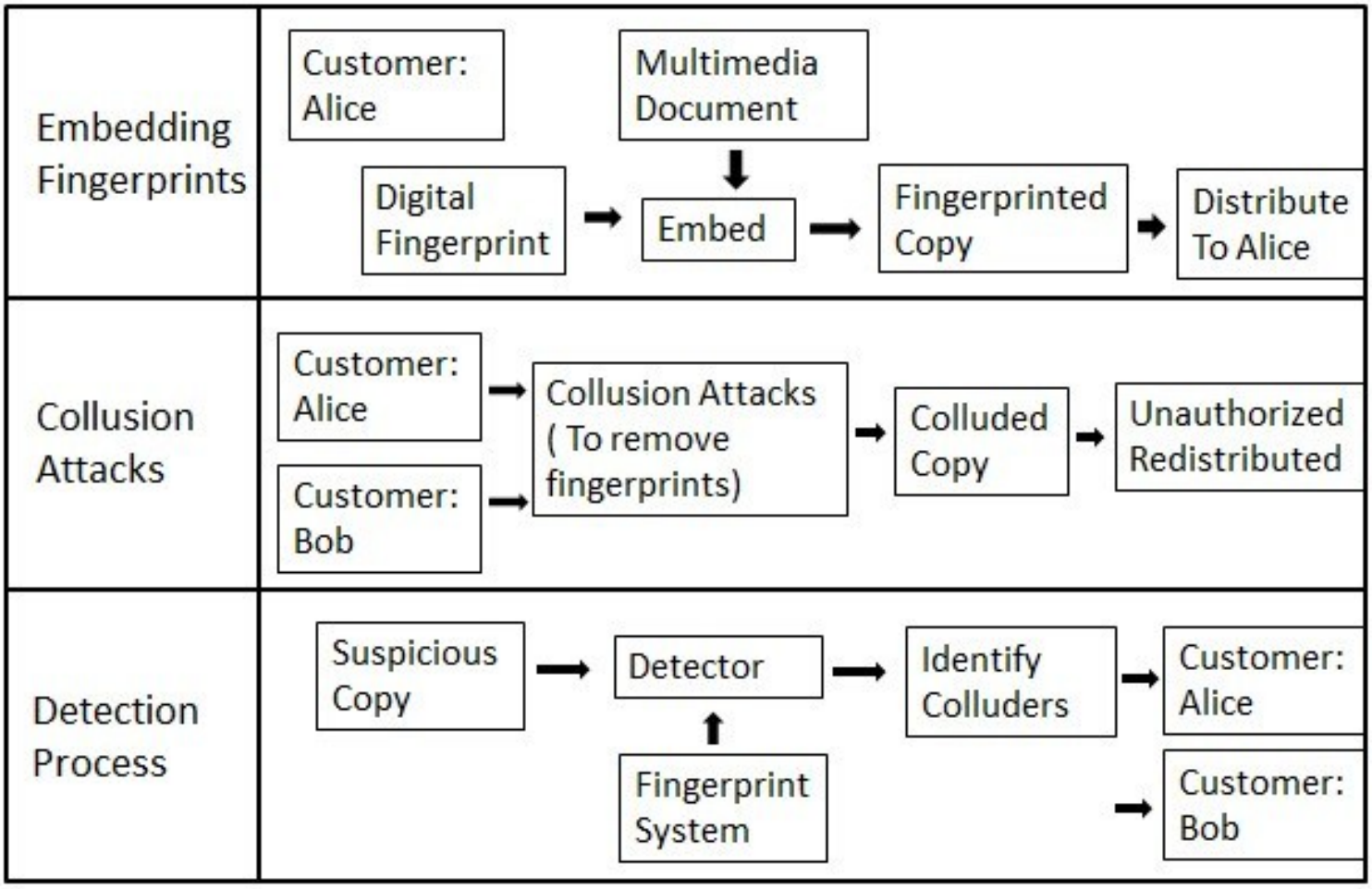


Figure 2.1: General Framework of Digital Fingerprinting System

which is called attacks. At the attackers' side, it is now easy for a group of users with different fingerprints to attack against the original content since two different fingerprinted copies can be compared and the differences between them detected. A simple and effective example of collusion attacks is average attacks, where each fingerprint energy is assigned the same weight $\frac{1}{K^2}$, K is the total number of colluders.

There are other different types of collusion attacks: attacks based on the median operation, attacks based on the minimum operations, and attacks based on the average of the minimum and maximum operations. Besides the multiuser collusion, one colluder can take single copy attack, for example, low pass filter and compression [42]. After collusion attacks, the colluded copy is illegally redistributed.

2.1.3 Detection Process

In the third stage, detection process is applied to trace and identify the colluders when the content owner finds out the existence of illegal distributions. Figure 2.1 shows that the content owner can extract the fingerprint and compare it to the existing fingerprints system to determine that whether the user is guilty or innocent. From the content owner's (detector's) point of view, there are two main detection scenarios: blind scenarios and nonblind scenarios [29], [30] depending on the presence of the host signal. A detection process fails if either the detector fails to identify a guilty user (false negative error) or an innocent user is found to be guilty (false positive error). A robust fingerprint design should maximize the possibility of successful detection and minimize the error probability.

2.2 Examples of Fingerprint Design

In this section, we introduce three examples of fingerprints system design: orthogonal fingerprints [25], simplex fingerprints [26] and Steiner ETF fingerprints [28], respectively.

2.2.1 Orthogonal Fingerprints

Orthogonal fingerprints are conceptually simple. The correlation between any two fingerprints is zero and thus can be ignored. In detection process, the orthogonality of fingerprints extremely helps the detector to reduce the probabilities of accusing an innocent user. In practice, the orthogonal Gaussian fingerprints are more popular. One method to achieve orthogonal

Gaussian fingerprints is to generate independent normally distributed random vectors and then orthogonalize them. From the view of colluders, orthogonal Gaussian fingerprints are very difficult to remove since the randomness of the fingerprints makes its system inherently resistant to collusion attacks. From the view of detector, the orthogonality is an important factor while the randomness has no consequences on detection results. Therefore, we use an identity matrix [27] to construct orthogonal fingerprints to simplify the process in our simulation. Table 2.1 presents an example of orthogonal fingerprints for 5 users using a 5×5 identity matrix.

Table 2.1: Orthogonal Fingerprints for 5 users

Users	1	2	3	4	5
	1	0	0	0	0
	0	1	0	0	0
	0	0	1	0	0
	0	0	0	1	0
	0	0	0	0	1

From Table 2.1, we can see that each column of the identity matrix is used as the fingerprint of each user. Every fingerprint is orthogonal to other fingerprints.

2.2.2 Simplex Fingerprints

Another optimal structure in coherence is the simplex fingerprints system. In [26], the author presented an additive fingerprints design. If the dimensions of the signal is N, the fingerprints system can apply more than N users while the orthogonal fingerprint system can only apply as much as N users. Moreover, the simplex fingerprints are maximally robust against Gaussian average collusion attacks, which maximize the probability of catching at least one colluder. Reliable detection is under the assumption that the number of colluders is far less than the length of the host signal. We give an example of simplex fingerprints applied to 6 users [37] in Table 2.2.

In Table 2.2, each column is one user's fingerprint and the dimension of signals is 5. The inner product of any two distinct fingerprints is $-\frac{1}{N} = 0.2$.

Table 2.2: Simplex Fingerprints for 6 users

Users	1	2	3	4	5	6
	1	-0.2000	-0.2000	-0.2000	-0.2000	-0.2000
	0	0.9797	-0.2449	-0.2449	-0.2449	-0.2449
	0	0	0.9486	-0.3162	-0.3162	-0.3162
	0	0	0	0.8944	-0.4472	-0.4472
	0	0	0	0	0.7745	-0.7745

Table 2.3: Block Design Parameters

Parameters	Definition
v	The number of elements of set
b	The number of the subset(blocks)
r	The number of blocks contains any element
k	The number of elements of the subset(blocks)
λ	The number of blocks contains any 2 fixed elements

2.2.3 ETF Fingerprints

Let $\mathbf{F} = \{\mathbf{f}\}_{m=1}^{M}$ be a finite sequence of fingerprints in a real N-dimensional space R_N. $\mathbf{F}$ is ETF fingerprints if $\| \mathbf{f}_m \| = 1$ and $| \langle \mathbf{f}_m, \mathbf{f}_{m'} \rangle | = \alpha$ for all $m /= m^{'}$, where $\alpha \geq 0$ [28]. Meanwhile, the fingerprints of $\mathbf{F}$ has unit norm and the inner products of any two distinct fingerprints of $\mathbf{F}$ is constant, which is called equiangular tight frames (ETF) fingerprints. Fickus, Mixon and Tremain proposed a method to construct ETF fingerprints using Steiner system.

In combinatorial mathematics, a Steiner system is a type of *block design*. More details of block design can be found in [31]-[32]. A Steiner system with parameters (v, b, r, k, λ) is written as $S(v, b, r, k, \lambda)$.

Table 2.3 shows that a v-element set V together with a collection of b, which is a set of k-element subset of V (called blocks), with the property that any element of V lies in exactly r blocks and that any 2-element subset of V is contained in λ blocks [28]. These parameters are not all independent, v, k, and λ determine b and r, and not all combinations of v, k, and λ are possible. There are two relations between the parameters: $vr = bk$ and $r(k-1) = \lambda(v-1)$, i.e., $r = \frac{v-1}{k-1}$ and $b = \frac{v(v-1)}{k(k-1)}$. In particular, $(2, k, v)$ Steiner system is involved in the construction of ETFs fingerprints, which has the property that 2-element subset of V is contained in the one block, that is, $\lambda = 1$.

The transpose $\{0, 1\}$ incidence matrix of a $(2, k, v)$ Steiner system is presented as $\mathbf{A}^T$, which is a $b \times v$ $(\frac{v(v-1)}{k(k-1)} \times v)$ matrix. The base matrix is used to generate an ETF fingerprints system consisting of $M = v(1 + \frac{v-1}{k-1})$ fingerprints in $N = \frac{v(v-1)}{k(k-1)}$-dimensional space, if there exists a real Hadamard matrix of size $1 + \frac{v-1}{k-1}$. Take $S(2, 3, 7)$ as an example, it consists of $b = 7$ blocks and each block consists of $k = 3$ elements. There are $v = 7$ elements in total and each element is contained in $r = 3$ blocks. Any two distinct elements are contained in exactly $\lambda = 1$ block. Correspondingly, its transpose $\{0, 1\}$ incidence matrix $\mathbf{A}^T$

$$\mathbf{A}^T = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Choose a 4×4 Hadamard matrix $\mathbf{H}$ to extend the base matrix $\mathbf{A}^T$. For each column, each nonzero entry is replaced by a distinct row of $\mathbf{H}$. In this example, we simply choose the second, third and fourth rows in order, which results in a real ETF fingerprint system $\mathbf{F}$ of $N = \frac{v(v-1)}{k(k-1)} = 7$ and $M = v(1 + \frac{v-1}{k-1}) = 28$. $\mathbf{F}$ is of the form

$$\mathbf{F} = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & & & & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & & & & \\ 1 & -1 & -1 & 1 & & & & 1 & 1 & -1 & -1 & & & & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ & & & & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & & & & 1 & 1 & -1 & -1 & & & & \\ & & & & 1 & -1 & -1 & 1 & & & & 1 & 1 & -1 & -1 & & & & & & 1 & 1 & -1 & -1 \\ & & & & & & & & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & & & & 1 & -1 & -1 & 1 \\ & & & & & & & & 1 & -1 & -1 & 1 & & & & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \end{bmatrix}$$

where $\frac{1}{\sqrt{3}}$ is the scaling factor [28].

The fingerprint system $\mathbf{F}$ can accommodate up to $M = 28$ users with the length of signals $N = 7$.

Compared to orthogonal and simplex fingerprints, Steiner equiangular tight frames (ETF) fingerprints can accommodate much more users ($M > N$) with comparable performance.

2.3 Performance Criteria

Different fingerprint systems have different properties, concerns and requirements. Basic assumptions and performance criteria should be set up before examining and comparing the performance of different digital fingerprint systems.

First, we assume that all the detection approaches are under a nonblind scenario. In a nonblind detection scenario, the host signal (original document) is known to the detector. On the other hand, in a blind scenario, the detector has no access to the host signal, which can be regarded as additional noise. Our research focuses on the nonblind scenario and the noise level is measured by watermark-to-noise ratio (WNR). The blind scenario can be considered as a nonblind scenario, which has a low WNR. In the following section, our simulation results show that the performance of fingerprint systems is related to WNR.

Second, the noise added to the fingerprinted copy is identical and independent Gaussian noise. In our simulations, the power of the noise is modulated by the requirement of WNR.

Catch one

In design of fingerprint systems, our general goal aims at catching colluders as much as possible while trying to reduce the probabilities of errors. In practice, some other concerns and evidences may be taken into consideration to design the fingerprint systems and make the final decision. In catch one scheme, there are mainly two components of the performance criteria, the probability of capturing at least one colluder P_d and the probability of accusing an innocent user P_{fa} [42].

The goal of catch one scheme is to maximize P_d and minimize P_{fa}, which can be applied to provide digital evidence to the court. From the view of detector, the detector has to succeed in catching at least one of the colluders and meanwhile not accusing any of the innocent users. Catch one scheme is widely used in the research works of digital fingerprinting. The requirements of catch one can be presented as

$$P_d \geq \varphi_d, \quad and \quad P_{fa} \leq \varphi_{fa} \tag{2.1}$$

where φ_d and φ_{fa} are determined by detector according to the purpose of detection.

Catch more

In the catch more scheme [42], the objective is to catch a certain fraction of colluders. In this case, the probability of accusing innocent users correspondingly increases. The components of performance criteria in this scheme include the fraction of successfully detected colluders $E[F_d]$ and the fraction of wrongly accused innocent users $E[F_{fa}]$. The requirements of catch more are

$$E[F_d] \geq \lambda_d, \quad and \quad E[F_{fa}] \leq \lambda_{fa} \tag{2.2}$$

where the parameters λ_d and λ_{fa} are properly chosen by detector according to the purpose of detection.

Catch all

In this scheme [42], the goal is to maximize the chances of catching all the colluders. Meanwhile, the probability of falsely accusing innocent users is kept at a low level. Catch all scheme is usually employed in the protection of highly confidential documents, the disclosure of which leads to serious consequences. It is crucial for the detector to catch all the colluders and fully prevent the illegal distribution. Let k be the number of colluders and M the number of total users. Then, the efficiency rate is defined as

$$R = \frac{(M - K) \times E[F_{fa}]}{K \times E[F_d]}. \tag{2.3}$$

Let $P_{d,all}$ be the probability of catching all the colluders. The requirements of catch all scheme are

$$R \leq \theta_r, \quad and \quad P_{d,all} \geq \lambda_d \tag{2.4}$$

where the parameters λ_d and θ_r are determined by detector.

In what follows, we introduce mathematical models of fingerprint scheme, attack model, and detection process.

2.4 Fingerprint Scheme and Attack Model

We assume that there are totally M users in the fingerprint system. The length of the signal is N, i.e., N-dimensional signal space. In order to avoid illegal distribution, a content owner embeds a *host signal* with fingerprints before distributing. The host signal is modeled as a vector $\mathbf{s} = (s_0, s_1, \cdots, s_{N-1})^T$,

where $s_i \in$ R, which is given to M users. Specifically, the mth user's fingerprinted copy is given by [27]

$$\mathbf{x_m} = \mathbf{s} + \mathbf{f_m} \tag{2.5}$$

where $\mathbf{f_m} = (f_0, f_1, \cdots, f_{N-1})^T$, $f_i \in$ R, denotes the mth fingerprint. Assume that the fingerprint has equal energy

$$\gamma^2 = \| \mathbf{f_m} \|^2 = N D_f \tag{2.6}$$

where D_f denotes the average energy per dimension of each fingerprint.

We consider an average collusion attack as shown in Figure 2.1, which were studied by most previous researches. Let K $\subseteq \{1, \cdots, M\}$ denotes a group of users who forge a copy of the host signal. Then, their averaging attack is of the form

$$\mathbf{y} = \sum_{k \in \mathrm{K}} \alpha_k (\mathbf{s} + \mathbf{f_k}) + \boldsymbol{\epsilon}, \qquad \sum_{k \in \mathrm{K}} \alpha_k = 1 \tag{2.7}$$

where $\boldsymbol{\epsilon}$ is a noise vector introduced by the colluders. In (2.7), α_k is the weight of kth colluder's copy in a forged copy and $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_M)$ is a vector of all the colluders' weights. Assume that $\boldsymbol{\epsilon}$ is a Gaussian noise with mean zero and variance σ^2, where σ^2 is the noise power per dimension. The strength of the attack noise is measured as the watermark to noise ratio (WNR), which is of the form

$$WNR = 10 \log_{10} \left(\frac{N D_f}{N \sigma^2} \right). \tag{2.8}$$

Note that (2.7) is the average linear attack model employed by us but it is worthy to mention other typical attack models. Assume that $\mathbf{y}^j_k = (\mathbf{s}^j + \alpha \mathbf{f}^j_k) + \boldsymbol{\epsilon}^j$, where $k \in$ K and $0 \leq j \leq N-1$. α is constant and j represents jth component of each fingerprinted copy, which is distributed to kth user. Then, minimum attack model, maximum attack model, median attack model, minmax attack model, modified negative attack model, and random negative attack model are presented as the following equations, from equation (2.9) to equation (2.14), respectively [42].

$$\mathbf{y}^j_{min} = (\mathbf{s}^j + \mathbf{f}^j_{min}) + \boldsymbol{\epsilon}^j, \qquad \mathbf{f}^j_{min} = \min(\{\mathbf{f}^j_k\} k \in \mathrm{K}) \tag{2.9}$$

$$\mathbf{y}^j_{max} = (\mathbf{s}^j + \mathbf{f}^j_{max}) + \boldsymbol{\epsilon}^j, \qquad \mathbf{f}^j_{max} = \max(\{\mathbf{f}^j_k\} k \in \mathrm{K}) \tag{2.10}$$

$$\mathbf{y}^j_{median} = (\mathbf{s}^j + \mathbf{f}^j_{median}) + \boldsymbol{\epsilon}^j, \qquad \mathbf{f}^j_{median} = \mathrm{median}(\{\mathbf{f}^j_k\} k \in \mathrm{K}) \tag{2.11}$$

$$\mathbf{y}^j_{minmax} = (\mathbf{y}^j_{min} + \mathbf{y}^j_{max})/2 \tag{2.12}$$

$$\mathbf{y}^j_{modneg} = \mathbf{y}^j_{min} + \mathbf{y}^j_{max} - \mathbf{y}^j_{median} \tag{2.13}$$

$$\mathbf{y}^j_{randneg} = \begin{cases} \mathbf{y}^j_{min}, & \text{with probability } p \\ \mathbf{y}^j_{max}, & \text{with probability } 1-p \end{cases} \tag{2.14}$$

where max(·), min(·), and median(·) denote maximize function, minimize function and median function.

Note that colluders may apply all the components of the fingerprinted copy to collude in practice since they are not aware of which components belong to the host signal.

2.5 Detection

A focused detection is used to decide whether a particular user is innocent or guilty. In the technical process, a focused detection computes a test statistic and performs a binary hypothesis test.

In this thesis, we assume a nonblind scenario that the host signal is available to the detector. Thus the host signal $\mathbf{s}$ can be subtracted from a forgery of (2.7), which yields

$$\mathbf{z} = \mathbf{y} - \mathbf{s} = \sum_{k \in \mathrm{K}} \alpha_k \mathbf{f_k} + \boldsymbol{\epsilon}. \tag{2.15}$$

The test statistic for the mth user is the normalized correlation function of $\mathbf{z}$ and the fingerprint, i.e.,

$$T_m(\mathbf{z}) = \frac{1}{\gamma^2} \langle \mathbf{z}, \mathbf{f_m} \rangle \tag{2.16}$$

where γ^2 is the fingerprint energy in (2.6).

For the mth user, let $H_1(m)$ denote the guilty hypothesis ($m \in$ K) and $H_0(m)$ the innocent

hypothesis ($m \notin$ K). With a correlation threshold τ, we use the following detector

$$\delta_m(\tau) = \begin{cases} H_1(m), & T_m(z) \geq \tau, \\ H_0(m), & T_m(z) < \tau. \end{cases} \tag{2.17}$$

The performance analysis of the focused detection is explicitly discussed in Chapter 4.

Chapter 3

New Fingerprint Design

In this chapter, a new fingerprint design using optical orthogonal codes is presented. This chapter is organized as follows. In Chapter 3.1, an introduction of optical orthogonal codes is given including its definition, construction and application. We review the construction of Steiner ETF fingerprints and discuss its potential drawbacks in Chapter 3.2. In Chapter 3.3, the core part of this chapter, we present constructions of the new fingerprint system using OOCs. The property of the coherence between any two distinct fingerprints is also given in this section. Then in Chapter 3.4, we have a review of modular Golomb Ruler and several constructions of it.

3.1 Optical Orthogonal Codes

Let $\mathbf{a} = (a_0, \cdots, a_{n-1})$ and $\mathbf{b} = (b_0, \cdots, b_{n-1})$ be a pair of binary sequences of period n, where each entry is 0 or 1. The *Hamming correlation* function [33] of the sequences is defined by $\theta_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{t=0}^{n-1} a_{t+\tau} b_t$, where $0 \leq \tau \leq n-1$ and $t+\tau$ is computed modulo n.

Definition 1 [34]: An (n, w, λ) *optical orthogonal code (OOC)* is a family of S binary sequences of period n, i.e., $\mathbf{F} = \{\mathbf{s}^{(i)} | 0 \leq i \leq S-1\}$. In the OOC family $\mathbf{F}$, each binary sequence has constant Hamming weight w and the Hamming autocorrelation satisfies $\theta_{\mathbf{s}^{(i)},\mathbf{s}^{(j)}} \leq \lambda$ for any (i, j) and for every τ, where $\tau \neq 0$ if $i = j$.

The application of multiple access fiber channels has motivated the study of OOCs. According to Definition 1, Hamming correlation between any two distinct sequences is low throughout. This property reduces the influences of disturbing signals. The thumb-shaped Hamming autocorrelation facilitates to

detect the target signal [33]. Except for multiple access channels domain, optical orthogonal codes are also used in mobile radio, radar, and spread spectrum communications.

Fan R.K concludes several methods to construct optical orthogonal codes. Iterative methods and greedy algorithm can be used to construct codes [33]. Both of the two methods yield lower bounds for code sizes. Constructions from finite projective geometries are a large class of optical orthogonal codes. Many of constructed codes have optimal structures. There are other methods to construct optical orthogonal codes, such as using block design and algebraic coding theory. There is a large amount of literatures in projective geometry filed. In this thesis, we use projective geometry tools to construct optical orthogonal codes, which are employed in our new fingerprint design. First, we cyclically shift codewords of an OOC to construct a base matrix. Then, a Hadamard matrix is employed to extend it and each column of the new matrix is used as one user's fingerprint.

3.2 Steiner ETF Fingerprints Design

In [28], Fickus, Mixon and Tremain presented Steiner equiangular tight frames using $(2, k, v)$ Steiner System. Our new fingerprint construction is derived from their construction. They used the transpose of the incidence matrix of a $(2, k, v)$ Steiner system to construct the base matrix, a $b \times v$ binary matrix that has k ones in each row and r ones in each column, and the inner product of any distinct column pair of the base matrix is 1. In [27] Fickus, Mixon, Quinn and Kiyavash used each column of the resulted matrix as each user's fingerprint to construct ETF fingerprints.

Steiner ETF fingerprints have two potential drawbacks. First, all nonzero entries $rv(\approx M)$ of the base matrix need to be remembered, which consumes storage when signal dimension N is great and the number of users M is large in practice. Second, They replaced each entry of one by a $(r+1) \times (r+1)$ Hadamard matrix. Then, there is a requirement of $r + 1 \equiv 0 \pmod 4$ to construct a real-valued frame. If we focus on the Steiner ETFs from affine and projective geometries [27], the requirement turns into $1 + \frac{q^n-1}{q-1} = q^{n-1} + q^{n-2} + \cdots + 2 \equiv 0 \pmod 4$, where q is a prime power and $n \geq 2$. Then, a possible choice for q and n meeting the requirement is either $q = 2$, or $q \equiv 1 \pmod 4$ and $n \equiv 3 \pmod 4$, which yields very few parameters for N and M [34].

Our new fingerprints construction is derived from Steiner ETF fingerprints construction but OOCs is used to construct the base matrix instead of Steiner system. Unlike Steiner ETF fingerprints, our new

design does not have to be optimal in coherence. Therefore, it has a more flexible structure and yields more parameters for N and M. For example, we use the Bose-Chowla method to yield a (q, q^2-1) Golomb ruler for any prime p, an positive integer n and $q = p^n$. The value of parameter N equals to $N = q^2 - 1 = p^{2n} - 1$. Affine geometries is used to construct a $(2, p, p^n)$ Steiner system for any prime p. Then, $N = b = \frac{v(v-1)}{k(k-1)} = \frac{p^n(p^n-1)}{p(p-1)} \approx p^{2(n-1)}$. For our new fingerprint design, any prime p and one positive integer n can yield one value of parameter N. However, for Steiner ETF fingerprints, p and n need to meet the requirements of $p = 2$, or $p \equiv 1 \pmod 4$ and $n \equiv 3 \pmod 4$, which results in fewer parameters.

3.3 New Fingerprints Using OOCs

Our fingerprint design is motivated to remedy the potential drawbacks of the Steiner ETF fingerprints. To provide more parameters for the fingerprint length and the number of users, and to allow efficient implementation with less storage, we construct new fingerprints using OOCs. In what follows, we assume that entries of the Hadamard matrix $\mathbf{H}$ are ± 1.

Construction 1 [34]: Let $\{\mathbf{s}^{(i)} | 0 \le i \le S-1\}$ be a set of S binary sequences obtained from an (n, w, λ) OOC. For each sequence $\mathbf{s}^{(i)}$, let $\Omega^{(i)} = \{d_0^{(i)}, \cdots, d_{w-1}^{(i)}\}$ be its support.

1) Cyclically shift each sequence $\mathbf{s}^{(i)}$ and arrange them as columns of a base matrix $\mathbf{B}$, where the support of the tth column of $\mathbf{B}$ is given by

$$\Delta_t = \{d_h^{(\lfloor \frac{t}{n} \rfloor)} - t \pmod n | h = 0, 1, \cdots, w-1\}$$

for $0 \le t \le nS - 1$. With $L = nS$, the $n \times L$ base matrix $\mathbf{B}$ is constructed with entries of 0 and 1. The Hamming weight of each column is w.

2) For small $\delta, 0 \le \delta < w$, define a positive integer $v = w + \delta$ such that $v \equiv 0 \pmod 4$. Then use a $v \times v$ Hadamard matrix $\mathbf{H}$ to extend the base matrix $\mathbf{B}$. In each column of $\mathbf{B}$, replace each entry of one by each distinct row of $\mathbf{H}$, and each entry of zero by all zero row of length v. The extension yields an $n \times vL$ matrix $\mathbf{B}_e = [\mathbf{B}_{e,1} | \cdots | \mathbf{B}_{e,L}]$, where $\mathbf{B}_{e,j}$ denotes an $n \times v$ submatrix extended from a single column of $\mathbf{B}$ for $0 \le j \le L-1$.

3) A new fingerprints system is given by $\mathbf{F} = \frac{1}{\sqrt{w}}\mathbf{B}_e = [\mathbf{F}_1 | \cdots | \mathbf{F}_L]$, where $\mathbf{F}_j = \frac{1}{\sqrt{w}}\mathbf{B}_e$, for $1 \le j \le L$. $\mathbf{F}$ has entries of 0 and $\pm \frac{1}{\sqrt{w}}$, and each column of $\mathbf{F}$ is used as each user's fingerprint. The

length of each fingerprint is $N = n$ and the total number of supported users is $M = vnS$.

In fact, Construction 1 has been originally presented in [34] for compressed sensing matrices, and is now applied in fingerprint design. In Construction 1, the coherence of $\mathbf{F}$ is defined as the maximum magnitude of inner products between a pair of distinct fingerprints, i.e., $\mu = \max_{i \neq j} \langle \mathbf{f_i}, \mathbf{f_j} \rangle$, where $\mathbf{f_i}$ and $\mathbf{f_j}$ are two distinct fingerprints of $\mathbf{F}$. The coherence of $\mathbf{F}$ is given by [34]

$$\mu \leq \max\left(\frac{\lambda}{w}, \frac{\delta}{w}\right).$$

Particularly, if $w = O(\sqrt{n})$ for small λ, $\delta = O(1)$, the fingerprints system $\mathbf{F}$ has the coherence of $O(\frac{1}{\sqrt{N}})$. In this case, our new fingerprints system does not have an optimal structure in coherence. However, simulation results show that its performance is only slightly worse than that of orthogonal and simplex fingerprints systems with optimal structures, which is demonstrated in Chapter 6.

In what follows, we present three example constructions of OOCs by employing modular Golomb rulers. In this thesis, we only employ Bose-Chowla construction [35] to construct OOCs. Then the resulted OOCs is used to construct our new fingerprints.

3.4 Modular Golomb Ruler

Definition 2 [34]: A (v, k) modular Golomb ruler is defined as a set of k integers $(d_0, \cdots, d_{k-1})$ such that all of the differences $\{d_i - d_j | 0 \leq i \neq j \leq k-1\}$ are distinct and nonzero modulo v.

Let G be a k element set where each element is in $\{0, 1, \cdots, v-1\}$. Define the *characteristic sequence* of G as $\mathbf{a} = (a_0, \cdots, a_{v-1})$, where

$$a_t = \begin{cases} 1, & \text{if } t \in G, \\ 0, & \text{if } t \notin G. \end{cases} \tag{3.1}$$

The set G is called the *support* of the characteristic sequence $\mathbf{a}$. If the set G is a (v, k) modular Golomb ruler, the Hamming autocorrelation satisfies $\theta_{\mathbf{a}}(\tau) \leq 1$ for any $\tau \neq 0$ and the Hamming weight of the characteristic sequence is k. Therefore, the characteristic sequence of a (v, k) modular Golomb ruler forms a $(v, k, 1)$ OOC with $S = 1$.

3.4.1 Bose-Chowla Construction

Definition 3 [35]: Let $q = p^m$ for prime p and a positive integer m. Let $GF(q) = \{0, 1, \beta, \beta^2, \cdots, \beta^{q-2}\}$, where $\beta^{q-1} = 1$, and β is a primitive element in $GF(q)$. Define

$$B = \{a : 1 \leq a < q^2 \text{ and } \beta^a - \beta \in GF(q)\}.$$

Then, B contains q integers which have distinct pairwise differences modulo $q^2 - 1$, so this yields a $(q^2 - 1, q)$ modular Golomb ruler.

Construction 1.1: Let $\mathbf{s}$ be the characteristic sequence of a $(q^2 - 1, q)$ modular Golomb ruler in Definition 1. Then $\mathbf{F} = \{\mathbf{s}\}$ is an $(n, w, 1)$ OOC of family size $S = 1$, where $n = q^2 - 1$ and $w = q$. Set $v = w + \delta \equiv 0 \pmod 4$ for small δ, $0 \leq \delta < w$. With the OOC and a $v \times v$ Hadamard matrix, Construction 1 gives an $N \times M$ fingerprints system with the following parameters.

1) $N = q^2 - 1$ and $M = vN$.

2) The coherence is $\mu = \frac{1}{q}$ if $\delta = 0$ for $q = 2^m$.

3) The density is $\frac{w}{N} \approx \frac{1}{q}$.

Table 3.1 shows the comparison of parameters between our new fingerprints design using Construction 1.1 and Steiner ETF fingerprints when N is no greater than 1000. The parameters of Steiner system are a complete set of parameters obtained from affine and projective geometries. The parameters of our new fingerprints are a complete set of parameters for Bose-Chowla construction. Our new fingerprint design can employ any kind of OOCs, which is not restricted to Bose-Chowla construction.

3.4.2 Singer Construction

Singer [38] proposed a $(q^2 + q + 1, q + 1, 1)$ perfect different set for the prime power q based on the projective geometry theory. The perfect difference set yields a $(q^2 + q + 1, q + 1, 1)$ modular Golomb ruler. Accordingly, a $(q^2 + q + 1, q + 1, 1)$ OOC can be constructed.

Construction 1.2: Let $\mathbf{s}$ be the characteristic sequence of a $(q^2 + q + 1, q + 1, 1)$ modular Golomb ruler where $q = p^m$ for prime p and a positive integer m. Then $\mathbf{F} = \{\mathbf{s}\}$ is an $(n, w, 1)$ OOC of family size $S = 1$, where $n = q^2 + q + 1$ and $w = q + 1$. Set $v = w + \delta \equiv 0 \pmod 4$ for small δ, $0 \leq \delta < w$. With the OOC and a $v \times v$ Hadamard matrix, Construction 1 gives an $N \times M$ fingerprints system with the following parameters.

Table 3.1: Comparison of Parameters between Steiner ETF and New fingerprint design

k	v	r	N	M
2	4	3	6	16
3	7	3	7	28
2	8	7	28	64
3	15	7	35	120
2	16	15	120	256
3	31	15	155	496
2	32	31	496	1024
3	63	31	651	2016
5	155	31	775	24800
6	156	31	806	25792
p	q	q^2-1	N	M
2	2	3	3	6
2	4	15	15	60
2	8	63	63	504
2	16	255	255	4080
3	3	8	8	32
3	9	80	80	640
3	27	728	728	20384
5	5	24	24	192
5	25	624	624	14976
7	7	48	48	384
11	11	120	120	1440
13	13	168	168	2688
17	17	288	288	5760
19	19	360	360	6480
23	23	528	528	12672
29	29	840	840	26880
31	31	960	960	30720

1) $N = q^2 + q + 1$ and $M = vNC_0 \leq vM$.

2) The coherence is $\mu = \max\left(\frac{1}{q+1}, \frac{\delta}{q+1}\right)$.

3) The density is $\frac{w}{N} \approx \frac{1}{q+1}$.

3.4.3 Rusza-Lindström Construction

Construction 1.3 uses a $(p^2-p, p-1)$ modular Golomb ruler from Rusza-Lindström Construction [39], [40] for every prime p. The specific examples of the construction can be found in Example 19.20 of [43] for $3 \leq p \leq 17$.

Construction 1.3: Let $\mathbf{s}$ be the characteristic sequence of a $(p^2-p, p-1)$ modular Golomb ruler

in Definition 3. Then $\mathrm{F} = \{\mathbf{s}\}$ is an $(n, w, 1)$ OOC of family size $S = 1$, where $n = p^2 - p$ and $w = p - 1$. Construction 1 gives an $N \times M$ fingerprints system with the following parameters

1) $N = p^2 - p$ and $M = vNC_0 \leq vM$.

2) The coherence is $\mu \leq \max\left(\frac{1}{p-1}, \frac{\delta}{p-1}\right)$. In particular, if $\delta = 0$ for $p \equiv 1 \mod (4)$, then $\mu \leq \frac{1}{p-1}$.

3) The density is $\frac{w}{N} = \frac{p-1}{p^2-p} = \frac{1}{p}$.

Chapter 4

Error Analysis

4.1 General Framework of Error Analysis

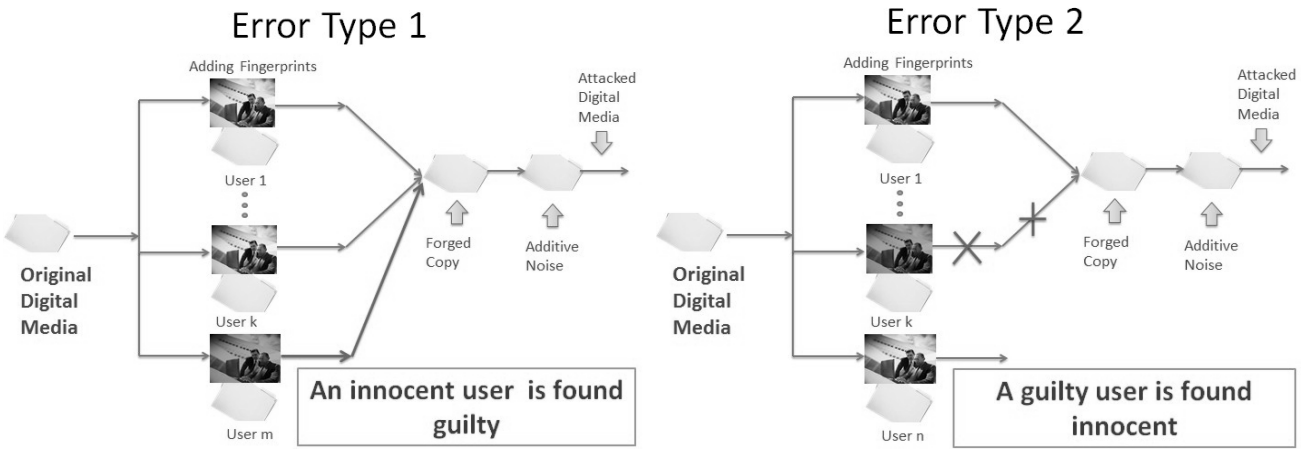
We analyze two types of errors for detection process, false positive error (type I) and false negative error (type II). The former is the probability $P_I(\mathbf{F}, m, \tau, \mathrm{K}, \boldsymbol{\alpha})$ that an innocent user $m (m \notin \mathrm{K})$ is found guilty ($T_m(z) \geq \tau$), which should be kept extremely low. The latter is the probability $P_{II}(\mathbf{F}, m, \tau, \mathrm{K}, \boldsymbol{\alpha})$ that a guilty user $m (m \in \mathrm{K})$ is found innocent ($T_m(z) < \tau$). They depend on the fingerprints $\mathbf{F}$, the coalition K, the weight vector $\boldsymbol{\alpha}$, and the threshold τ. The formulations of error analysis in [27] are summarized in Table 4.1. The models for Error type I and II are shown in Figure 4.1.

In Table 4.1, $P_I(\mathbf{F}, \tau, \boldsymbol{\alpha})$ and $P_{II}(\mathbf{F}, \tau, \boldsymbol{\alpha})$ are the worst case probabilities of type I and type II, respectively, which are analyzed further in Theorem 1. The worst case error probability is defined as the maximum of these two error probabilities, i.e.,

$$P_e(\mathbf{F}, \tau, \boldsymbol{\alpha}) = \max\{P_I(\mathbf{F}, \tau, \boldsymbol{\alpha}), P_{II}(\mathbf{F}, \tau, \boldsymbol{\alpha})\}.$$

Table 4.1: Formulations of Error Analysis

False positive error	False negative error
$P_I(\mathbf{F}, m, \tau, \mathrm{K}, \boldsymbol{\alpha}) = Prob[T_m(z) \geq \tau \mid H_0(m)]$	$P_{II}(\mathbf{F}, m, \tau, \mathrm{K}, \boldsymbol{\alpha}) = Prob[T_m(z) < \tau \mid H_1(m)]$
$P_{fa}(\mathbf{F}, \tau, \mathrm{K}, \boldsymbol{\alpha}) = \max_{m \notin \mathrm{K}} P_I(\mathbf{F}, m, \tau, \mathrm{K}, \boldsymbol{\alpha})$	$P_m(\mathbf{F}, \tau, \mathrm{K}, \boldsymbol{\alpha}) = \min_{m \in \mathrm{K}} P_{II}(\mathbf{F}, m, \tau, \mathrm{K}, \boldsymbol{\alpha})$
$P_I(\mathbf{F}, \tau, \boldsymbol{\alpha}) = \max_{\mathrm{K}} P_{fa}(\mathbf{F}, \tau, \mathrm{K}, \boldsymbol{\alpha})$	$P_{II}(\mathbf{F}, \tau, \boldsymbol{\alpha}) = \max_{\mathrm{K}} P_m(\mathbf{F}, \tau, \mathrm{K}, \boldsymbol{\alpha})$
-	$P_d(\mathbf{F}, \tau, \mathrm{K}, \boldsymbol{\alpha}) = 1 - P_m(\mathbf{F}, \tau, \mathrm{K}, \boldsymbol{\alpha})$



(a) WNR=0 dB (b) WNR=2.5 dB

Figure 4.1

The threshold parameter τ can be varied to minimize this quantity, yielding the minmax error probability

$$P_{minmax}(\mathbf{F}, \boldsymbol{\alpha}) = \min_{\tau} P_e(\mathbf{F}, \tau, \boldsymbol{\alpha})$$

which will be bounded in Theorem 1.

4.2 Error Analysis of New Fingerprints

In this section, we further discuss the two types of error probability using the new fingerprints design.

Theorem 1: Recall γ and σ in Chapter 2. Consider a fingerprints system $\mathbf{F} = \{\mathbf{f_m}\}_{m=1}^{M}$, where each fingerprint has the length of N. Then, the worst case probabilities of type I and type II error satisfy

$$P_I(\mathbf{F}, \tau, \boldsymbol{\alpha}) \leq Q[\frac{\gamma}{\sigma}(\tau - \mu')]$$

$$P_{II}(\mathbf{F}, \tau, \boldsymbol{\alpha}) \leq Q[\frac{\gamma}{\sigma}(((1+\mu')\max_{k\in \mathrm{K}} \alpha_k - \mu') - \tau)]$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} e^{(\frac{-2u^2}{})} du$. In Construction 1, $\mu' = \max(\frac{\lambda}{w}, \frac{\delta}{w})$ while $\mu' = \frac{1}{q}$ for Construction 1.1.

Proof: Under innocent hypothesis $H_0(m)$, ($m \notin$ K). The test statistic for mth user is

$$\begin{aligned} T_m(z) &= \frac{1}{\gamma^2}\langle \sum_{n\in \text{K}} \alpha_n \mathbf{f_m} + \boldsymbol{\epsilon}, \mathbf{f_m} \rangle \\ &= \sum_{n\in \text{K}} \alpha_n \langle \mathbf{f_n}, \mathbf{f_m} \rangle + \varepsilon' \\ &= \sum_{n\in \text{K}} \alpha_n c_n + \varepsilon' \end{aligned}$$

where c_n is the coherence of $\mathbf{f_n}$ and $\mathbf{f_m}$, which has three possible values $-\mu'$, 0 and μ'. Recall Construction 1, if $\mathbf{f_n}$ and $\mathbf{f_m}$ are from the same subsystem $\mathbf{F}_j$, for $1 \le j \le N-1$, c equals to $-\mu'$ or μ'. Otherwise, it equals to 0. ε' is the projection of the noise to the fingerprint

$$\varepsilon' \sim N(0, \frac{\sigma^2}{\gamma^2})$$

So

$$T_m(z) \sim N(\sum_{n\in \text{K}} \alpha_n c_n, \frac{\sigma^2}{\gamma^2})$$

Thus, we can subtract the mean and divide by the standard deviation to obtain

$$Prob[T_m(z) \ge \tau] = Q[\frac{\gamma}{\sigma}(\tau - (\sum_{n\in \text{K}} \alpha_n c_n))]$$

where $\sum_{k\in \text{K}} \alpha_k = 1$ and $\max \sum_{n\in \text{K}} \alpha_n c_n = \sum_{n\in \text{K}} \alpha_n \mu' = \mu'$. We can also obtain the upper bound of $P_I(\mathbf{F}, \tau, \boldsymbol{\alpha})$

$$Prob[T_m(z) \ge \tau] \le Q[\frac{\gamma}{\sigma}(\tau - \mu')]$$

Likewise, under guilty hypothesis $H_1(m)$, ($m \in$ K). The test statistic for mth user is

$$\begin{aligned} T_m(z) &= \frac{1}{\gamma^2}\langle \sum_{n\in \text{K}} \alpha_n \mathbf{f_n} + \boldsymbol{\epsilon}, \mathbf{f_m}\rangle \\ &= \sum_{n\in \text{K}} \alpha_n \langle \mathbf{f_n}, \mathbf{f_m}\rangle + \varepsilon^{'} \\ &= \alpha_m \langle \mathbf{f_m}, \mathbf{f_m}\rangle + \sum_{n\in \text{K}\setminus\{m\}} \alpha_n \langle \mathbf{f_n}, \mathbf{f_m}\rangle + \varepsilon^{'} \\ &= \alpha_m + \sum_{n\in \text{K}\setminus\{m\}} \alpha_n c_n + \varepsilon^{'}. \end{aligned}$$

So

$$T_m(z) \sim N(\alpha_m + \sum_{n\in \text{K}\setminus\{m\}} \alpha_n c_n, \frac{\sigma^2}{\gamma^2}).$$

Since $1 - Q(x) = Q(x)$, the type II error probability can be bounded as

$$\begin{aligned} Prob[T_m(z) \le \tau] &= Q(-\frac{\gamma}{\sigma}[\tau - (\alpha_m + \sum_{n\in \text{K}\setminus\{m\}} \alpha_n c_n)]) \\ &\le Q(-\frac{\gamma}{\sigma}[\tau - (\alpha_m + \sum_{n\in \text{K}\setminus\{m\}} \alpha_n \mu^{'})]) \\ &= Q(\frac{\gamma}{\sigma}([\alpha_m(1+\mu^{'}) - \mu^{'}] - \tau)). \end{aligned}$$

We can further maximize over all possible weightings $\boldsymbol{\alpha}$

$$\begin{aligned} P_I(\mathbf{F}, \tau) &= \max_{\boldsymbol{\alpha}} P_I(\mathbf{F}, \tau, \boldsymbol{\alpha}) \\ &\le Q[\frac{\gamma}{\sigma}(\tau - \mu^{'})] \\ P_{II}(\mathbf{F}, \tau) &= \max_{\boldsymbol{\alpha}} P_{II}(\mathbf{F}, \tau, \boldsymbol{\alpha}) \\ &\le \max_{\boldsymbol{\alpha}} Q[\frac{\gamma}{\sigma}(\max_{m\in \text{K}} \alpha_m(1+\mu^{'}) - \mu^{'}] - \tau)] \\ &= Q[\frac{\gamma}{\sigma}(\min_{\boldsymbol{\alpha}} \max_{m\in \text{K}} \alpha_m(1+\mu^{'}) - \mu^{'}] - \tau)] \\ &= Q[\frac{\gamma}{\sigma}(\frac{1}{K}(1+\mu^{'}) - \mu^{'}] - \tau)]. \end{aligned}$$

The uniform weight vector $\boldsymbol{\alpha}$ minimizes the value of α_m, i.e., maximizes the probability of not catching any colluders. Linear average attack model is widely studied in prior works.

Theorem 2: Recall D_f, the minmax error probability can be bounded as

$$Q(\frac{d^*_{low}}{2}) \leq P_{minmax}(\mathbf{F}, \boldsymbol{\alpha}) \leq Q(\frac{d^*_{up}}{2}) \tag{4.1}$$

where

$$d^*_{low} = \frac{\sqrt{\frac{M}{M-1}}\sqrt{N D_f}}{\sigma\sqrt{K(K-1)}}$$

$$d^*_{up} = \frac{\sqrt{N D_f}}{\sigma K}(1-(2K-1)\mu),$$

where K is the number of colluders.

The proof of Theorem 2 is similar to that of [27].

Proof: The lower bound is the sphere packing lower bound introduced in [45]. For the upper bound

$$\begin{aligned} P_e(\mathbf{F}, \tau, \boldsymbol{\alpha}) &= \max\{P_I(\mathbf{F}, \tau, \boldsymbol{\alpha}), P_{II}(\mathbf{F}, \tau, \boldsymbol{\alpha})\} \\ &\leq \max\{Q[\frac{\gamma}{\sigma}(\tau - \mu')], Q[\frac{\gamma}{\sigma}(((1+\mu')\max_{k\in \mathrm{K}} \alpha_k - \mu') - \tau)]\}. \end{aligned}$$

The test statistic is normally distributed with the same variance under either the guilty hypothesis or the guilty hypothesis,the value of threshold τ that minimizes the upper bound is the average of μ' and $\frac{1+\mu'}{K} - \mu'$, that is, $\tau^* = \frac{1+\mu'}{2K}$. Using this τ^*, we have

$$\begin{aligned} P_{minmax}(\mathbf{F}, \boldsymbol{\alpha}) &= \min_{\tau} P_e(\mathbf{F}, \tau, \boldsymbol{\alpha}) \\ &= P_e(\mathbf{F}, \tau^*, \boldsymbol{\alpha}) \\ &\leq Q(\frac{\gamma}{\sigma}(\tau^* - \mu')) \\ &= Q(\frac{\sqrt{N D_f}}{\sigma K}(1-(2K-1)\mu')) \\ &= Q(\frac{d^*_{up}}{2}) \end{aligned}$$

Chapter 5

Fast Processing

Chapter 5 is divided into two sections. The first section introduces fast processing in detection using the property that only part of the entries are nonzero entries in the new fingerprint system. This property reduces the computational complexity, which will be presented in theory. Then, Inverse Fast Hadamard Transform (IFHT) [36] is employed to reduce the computational complexity further. The second section introduces the application of IFHT for fast processing.

5.1 Fast Processing In Detection

This section describes how to apply the fast processing technique in detection process for our new fingerprint design. In Construction 1, a $v \times v$ Hadamard matrix is used to extend each column of the base matrix. In this way, there are w nonzero entries for each fingerprint of length N from which the computational complexity can be reduced, since only the nonzero entries in each fingerprint are involved in the detection process. In this section, we discuss a fast detection for the fingerprints presented in Construction 1.1. It is a particular example of Construction 1 when the number of cyclically distinct binary sequences equals to 1 ($S = 1$). Then, the fast detection process for Construction 1 can be easily extended by the detection process for Construction 1.1.

In Construction 1.1, all the users' fingerprints system is presented as $\mathbf{F} = [\mathbf{f}_1|\mathbf{f}_2|\cdots|\mathbf{f}_M]$, where each column $\mathbf{f}_i$ represents the ith user's fingerprint, where $1 \leq i \leq M$. The length of the fingerprint is N and M users are accommodated in total. Recall that the support of the first column of the base matrix

is $\mathbf{d}^{(0)} = \{d_0^{(0)}, \cdots, d_{w-1}^{(0)}\}$ and the support of the nth column of the base matrix is

$$\mathbf{d}^{(n)} = \{d_t^{(0)} - n \pmod N | t = 0, 1, \cdots, w-1\} \tag{5.1}$$

where $0 \leq n \leq N-1$ and w is the Hamming weight.

In the fingerprints $\mathbf{F}$, let us define an $N \times v$ subsystem $\mathbf{F}_n = [\mathbf{f}_{(n-1)v} | \cdots | \mathbf{f}_{nv-1}]$, where $\mathbf{F} = [\mathbf{F}_1 | \cdots | \mathbf{F}_N]$. In Construction 1.1, all the nonzero entries of $\mathbf{F}_n$ form a $w \times v$ matrix $\frac{1}{\sqrt{w}}\mathbf{H}$, where $\frac{1}{\sqrt{w}}\mathbf{H} = \frac{1}{\sqrt{w}}[\mathbf{h}_1 | \cdots | \mathbf{h}_v]$, $\mathbf{h}_i$ is the ith column of $\mathbf{H}$, $1 \leq i \leq v$. Each row of $\mathbf{H}$ is from a $v \times v$ Hadarmard matrix. Moreover, the fingerprints of $\mathbf{F}_n$ share the same support $\mathbf{d}^{(n)}$ in (5.1) as they are from a single sequence. In detection process, let the $((n-1)v + j)$th user's test statistic be $t_{(n-1)v+j}$, where $0 \leq j \leq v-1$. (2.16) implies that $t_{(n-1)v+j}$ is the normalized correlation function of the fingerprint $\mathbf{f}_{(n-1)v+j}$ and $\mathbf{z}$ in (2.15). In order to reduce the computational complexity, the nonzero entries are abstracted from $\mathbf{f}_{(n-1)v+j}$ and thus $t_{(n-1)v+j}$ can be written as

$$t_{(n-1)v+j} = \frac{1}{\gamma^2}\frac{1}{\sqrt{w}}\langle \mathbf{h}_{j+1}, \mathbf{z}_{\mathbf{d}^{(n)}} \rangle, \quad 0 \leq j \leq v-1$$

where $\mathbf{z}_{\mathbf{d}^{(n)}}$ is a $w \times 1$ vector, which takes only w entries of $\mathbf{z}$ with the same support $\mathbf{d}^{(n)}$.

Then, a $v \times 1$ vector $\mathbf{t}_n = [t_{(n-1)v}, \cdots, t_{nv-1}]^T$, a set of test statistics of v users having their fingerprints $\{\mathbf{f}_{(n-1)v}, \cdots, \mathbf{f}_{nv-1}\}$, can be computed as

$$\mathbf{t}_n = \frac{1}{\gamma^2}\frac{1}{\sqrt{w}}\mathbf{I}^{-T}\mathbf{z}_{\mathbf{d}^{(n)}}. \tag{5.2}$$

From (5.2), the matrix-vector multiplication has the computational complexity of $O(v^2)$. Therefore, the computational complexity of all the users' test statistics turns out to be $O(v^2 N)$, that is, $O(vM)$. If we employ the Inverse Fast Hadamard Transform technique for (5.2), the computational complexity will be reduced from $O(vM)$ to $O(M \log_2 v)$. In practice, the fast processing technique will improve the speed of detection and construction.

5.2 Inverse Fast Hadamard Transform

In Chapter 5.1, we present fast processing in detection. In equation (5.2), all the nonzero entries are abstracted to form a $w \times 1$ vector multiplied by a partial transposed Hadamard matrix. In essence, the

process of the multiplication is the partial Inverse Hadamard Transform of an input vector, where the input vector is $\mathbf{z}_{\mathbf{d}^{(n)}}$ and the output vector is $\mathbf{t}_n$. In this section, we introduce how to further reduce the computational complexity based on partial Inverse Hadamard Transform. First, we give the definition of a Hadamard matrix. Then, we present how to convert the partial Inverse Hadamard Transform to Inverse Hadamard Transform. In the last part of the section, we use the introduced definition of Hadamard matrix to explain the process of Inverse Fast Hadamard Transform (IFIT) [36].

The Inverse Hadamard Transform [36] is an example of generalized class of Fourier transforms, which is a $2^p \times 2^p$ matrix scaled by a normalization factor $\frac{1}{\sqrt{2^p}}$. It performs an orthogonal, symmetric, linear operation on 2^p real numbers. The Hadamard matrix is in fact equivalent to a multidimensional DFT of size $2 \times 2 \times 2 \times 2 \cdots \times 2$. It decomposes an arbitrary vector into a superposition of Walsh Functions. First, we give the definition of the Hadamard matrix. In this thesis, we use the binary representation of the indices n and k to define each entry of a Hadamard matrix [44]. The binary representation of the indices n and k is of the form

$$k = \sum_{i=0}^{p} k_i 2^i = k_{p-1}2^{p-1} + k_{p-2}2^{p-2} + \cdots + k_1 2 + k_0 \tag{5.3}$$

$$n = \sum_{i=0}^{p} n_i 2^i = n_{p-1}2^{p-1} + n_{p-2}2^{p-2} + \cdots + n_1 2 + n_0 \tag{5.4}$$

where the k_i and n_i are the binary digits (0 or 1) of k and n for the component 2^i. In a Hadamard matrix, we define the indices of the entry in the top left corner as the $(0, 0)th$ entry. We have the definition of the $(k, n)th$ entry

$$H_v(k, n) = \frac{1}{2^{\frac{v}{2}}}(-1)^{\sum_{j=0}^{p} k_j n_j}. \tag{5.5}$$

One example of such a Hadamard matrix follows

$$\mathbf{H}_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \tag{5.6}$$

In (5.5), $\sum_{j=0}^{j<p} k_j n_j$ is the product of the binary representations of the indices k and n. For example, if $v = 8$, then $H_v(3, 2) = (-1)^{3\times 2} = (-1)^{(1,1)\cdot(1,0)} = (-1)^{1+0} = -1$ [44].

Before employing Inverse Fast Hadamard Transform (IFHT), we need to change the $v \times w$ partial transposed Hadamard matrix $\mathbf{H}^T$ to $v \times v$ transposed Hadamard matrix $\mathbf{H}^T_v$. We can construct $\mathbf{H}^T_v$ by adding $\mathbf{c}_w, \cdots, \mathbf{c}_{v-1}$ to $\mathbf{H}^T$, where $\mathbf{c}_i$ is the $(i)th$ column of $\mathbf{H}^T_v$, $w \le i \le v-1$. The $(n, k)th$ entry of $\mathbf{H}^T_v$ is defined as $H_v(n, k)$, where $n = 0, 1, \cdots, v-1$ and $k = 0, 1, \cdots, v-1$. The forged copy (input vector) $\mathbf{z}_u(g)$ is changed from a $w \times 1$ vector to a $v \times 1$ vector by adding zero entries of $z(w), \cdots, z(v-1)$. The entries of the input vector are $z(k)$, $k = 0, 1, 2, \cdots, v-1$. Thus, the partial transposed Inverse Hadamard matrix is changed to Inverse Hadamard matrix.

From the point of Inverse Hadamard Transform (IHT), Inverse Fast Hadamard Transform (IFHT) is a more efficient way of computation. IFHT can be employed in our fast processing technique to further reduce the computational complexity. In what follows, we introduce the theoretical derivation of its application in fast processing technique. We can break down the IHT of the input vector with v points to the operation of two components, which are the IHTs of two subvectors with $\frac{v}{2}$ points. We do the same thing to the resulted IHTs until the component is the IHT of one point. Usually inverse Hadamard transform would have a computational complexity of $O(v^2)$ and IFHT only requires $O(v \log_2 v)$. Assume that the entries of the output vector are $t(n)$, $n = 0, 1, 2, \cdots, v-1$, where $v = 2^p$.

Equation (5.2) can be computed as

$$
\begin{aligned}
t_n &= \sum_{k=0}^{v-1} H_v(n,k)\cdot z(k) \\
&= \frac{1}{\gamma^2\sqrt{w}} \sum_{k=0}^{v-1} (-1)^{\sum_{j=0}^{j<p} k_j n_j} \cdot z(k) \\
&= \frac{1}{\sqrt{w}} \sum_{l=0}^{\frac{v}{2}} (-1)^{\sum_{j=0}^{j<p} l_j n_j} \cdot z(l) + \frac{1}{\gamma^2\sqrt{w}} \sum_{l=\frac{\bar{2}}{v}+1}^{v-1} (-1)^{\sum_{j=0}^{j<p} l_j n_j} \cdot z(l) \\
&= T_{\frac{v}{2}} z(k) + (-1)^{k'} T_{\frac{v}{2}} z(k)
\end{aligned}
\tag{5.7}
$$

where $T_{\frac{v}{2}}$ is the transform of the subvector with the length of $\frac{v}{2}$ points. k' is the one of the binary digit, that is $k' = p-1, p-2, \cdots 0$. In (5.7), $k' = p-1$.

Similarly, we divide the IHT of the subvectors with $\frac{v}{2}$ points into the operation of the IHTs of the subvectors with $\frac{v}{4}$ points until we compute the IHT of only one point. For each entry of the output vector, the computational complexity is $O(\log_2 v)$ and thus for the v entries, the computational complexity is $O(v \log_2 v)$. In this way, the computational complexity of new fingerprints is reduced from $O(N M)$ to $O(M \log_2 v)$.

Chapter 6

Simulation Results

In order to measure the robustness of different fingerprint systems, we compare the maximum number of colluders which can be tolerated. We plot the probability of detecting at least one colluder P_d as a function of the number of colluders K. The threshold τ is picked to guarantee reasonably low P_{fa}. With the given P_{fa}, we can explore the number of colluders required for an average attack with high undetected probability. We assume the fingerprint system requires $P_d \geq 0.8$ and $P_{fa} \leq 10^{-3}$ [5] since high P_d and low P_{fa} are necessary to guarantee the systems' robustness.

In this section, we compare the performance of orthogonal, simplex and new fingerprint systems for $N = \{63, 255, 1023, 4095\}$. For orthogonal fingerprints, we use each column of an identity matrix as one user's fingerprint, where the total number of users equals to $M = N$. We use simplex fingerprints having the same power (γ) and having the same inner product ($-\frac{1}{N}$) [37], where $M = N + 1$. Our construction is from Construction 1.1, where $q = 64$, $\delta = 0$, $v = q$, and $M = vN$. While N and $N + 1$ users are accommodated by orthogonal and simplex fingerprints, respectively, our fingerprints can support much more users up to vN about v times more.

Total 3000 average attacks were simulated for each fingerprint system and collusion size K. We randomly choose colluders and uniformly average their copies to form a forgery. The Gaussian noise with power σ^2 per dimension is added to the forged copy. We pick a threshold τ to ensure $P_{fa} = 10^{-3}$. For each attack, we measure P_d by detecting every user in the fingerprint system.

The simulations are divided into four groups. In the first group, we test the performance of orthogonal, simplex and new fingerprints for $N = 63$ and WNR=$\{-5, -2.5, 0, 2.5, 5\}$dB, respectively. The

results are exhibited in Figure 6.1. Clearly, Figure 6.1 shows that P_d approaches 0 when the number of colluders increases. The weight (contribution) of each colluder to the forged copy becomes smaller when more and more colluders are involved in an average attack. The test statistic of one colluder's copy and the forged copy is also decreased. Put it in an extreme case, there is obviously no difference existing in test statistics when all the users are colluders. We can observe the same trend in all the three different fingerprints systems.

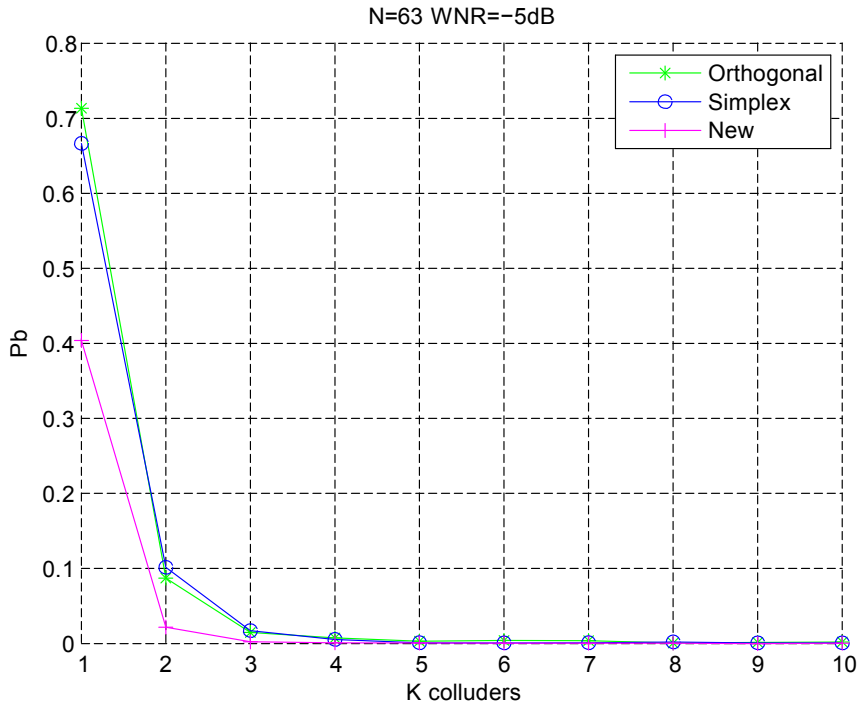
63, 64 and 504 users can be accommodated by orthogonal, simplex and our new fingerprints in the first group simulations. The maximum number of colluders that can be tolerated is similar and approximately one more than our new fingerprint system in Figure 6.1 (c) and (d) and two more in Figure 6.1 (e). Overall, the maximum number of colluders that can be tolerated by a fingerprints system is very small since the dimension of the fingerprints is only 63. From Figure 6.1 (a) to (e), we can observe that the performance gap between our new fingerprints and the other two fingerprints becomes smaller when the noise level increases.

In the following three groups of simulations, we also compare the performances of orthogonal, simplex and new fingerprints for WNR=$\{-5, -2.5, 0, 2.5, 5\}$dB, where the dimensions of the fingerprints are $\{255, 1023, 4095\}$, respectively. Figure 6.2 shows the result of the second group of simulations, where 255, 256 and 4080 users can be accommodated by orthogonal, simplex and our new fingerprints. In Figure 6.2, the observations are similar to Figure 6.1 while the maximum number of colluders that can be tolerated increases when the dimension increases from 63 to 255. This trend is more obvious when the dimension is 1023 and 4095 much greater than 63, which can be observed in Figure 6.3 and 6.4.

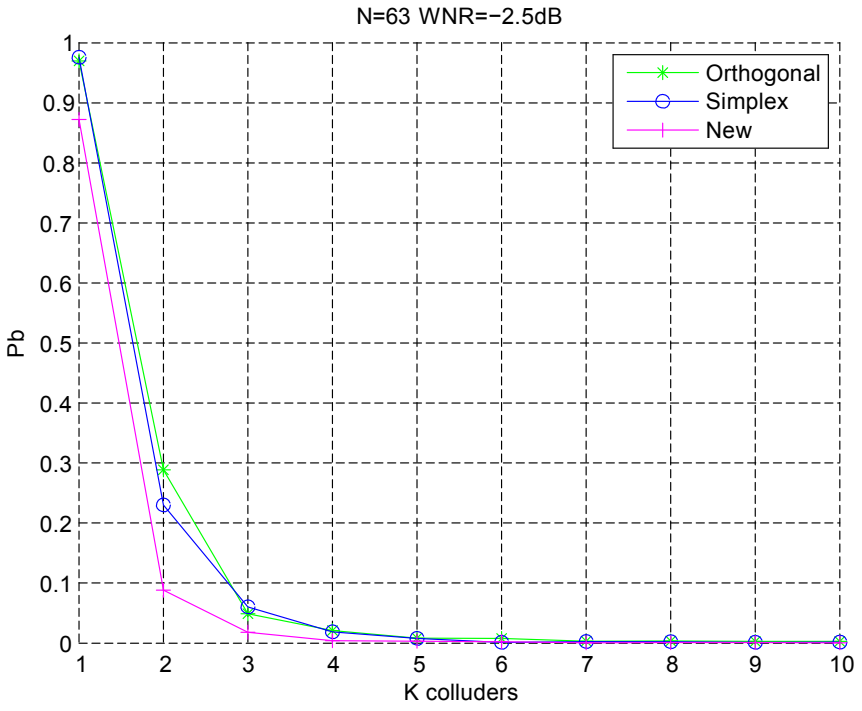
1023 and 1024 users can be accommodated by orthogonal and simplex fingerprints with the length $N = 1023$. 4095 and 4096 users can be accommodated by orthogonal and simplex fingerprints with the length $N = 4095$. In theory, up to 32736 and 262080 users can be accommodated by our fingerprints with the length $N = 1023$ and $N = 4095$, respectively. Due to technical limitations in simulation, 16368 and 32768 users' fingerprints are simulated.

The important fact that the gap between our new fingerprints and the other two fingerprints with the same noise level is getting smaller can be observed by comparing Figure 6.1 (c), 6.2 (c), 6.3 (c) and 6.4 (c), where the dimensions of the signals are $\{63, 255, 1023, 4095\}$. We have the similar observation when the noise level changes. The coherence of our new fingerprint design is no less than that of orthogonal

and simplex fingerprints. Overall, our new fingerprints perform slightly worse than orthogonal and simplex fingerprints in P_d while accommodating much more users.

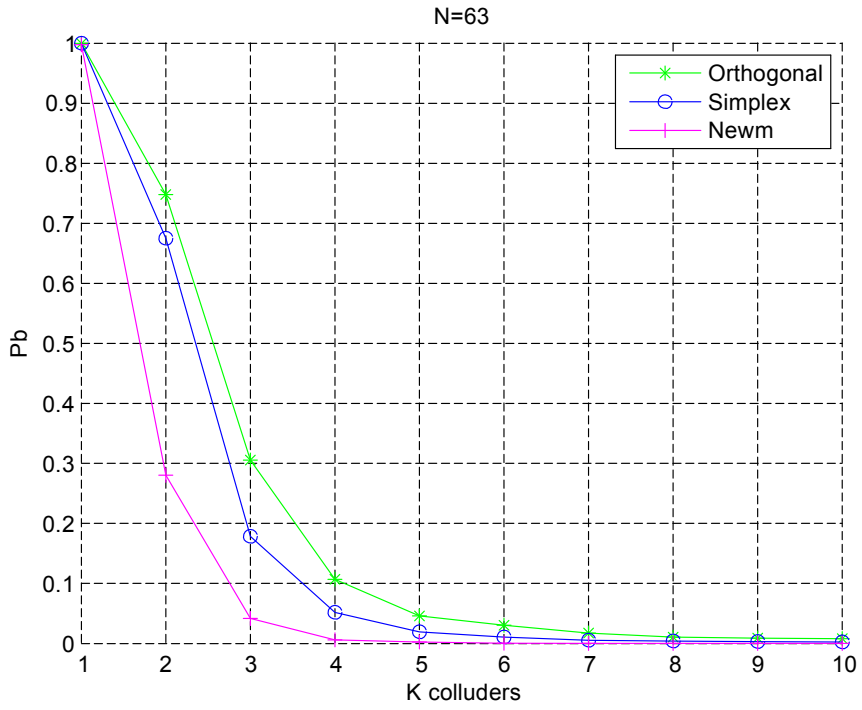


(a) WNR=-5 dB

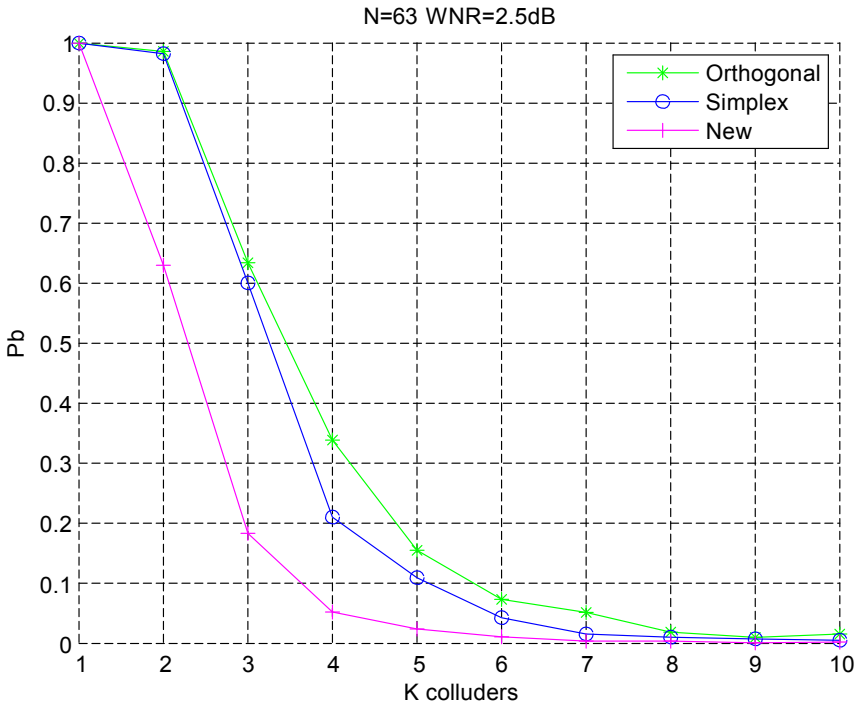


(b) WNR=-2.5 dB

Figure 6.1

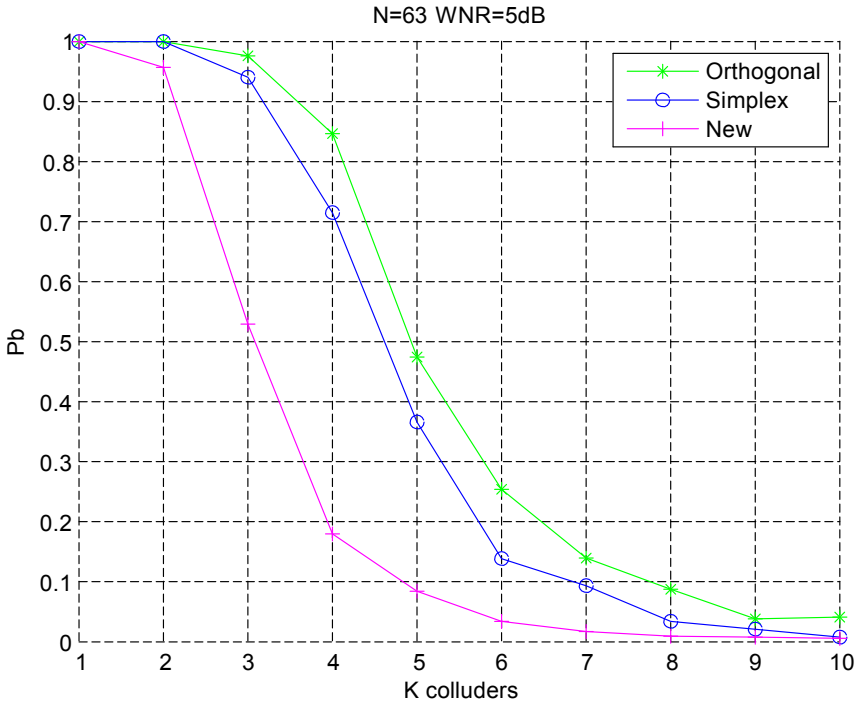


(c) WNR=0 dB



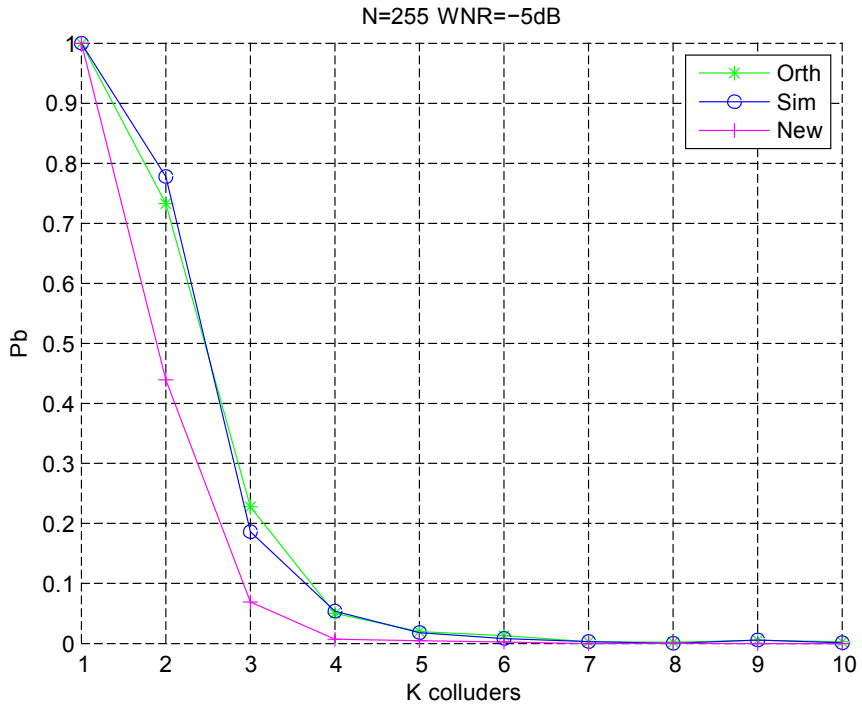
(d) WNR=2.5 dB

Figure 6.1

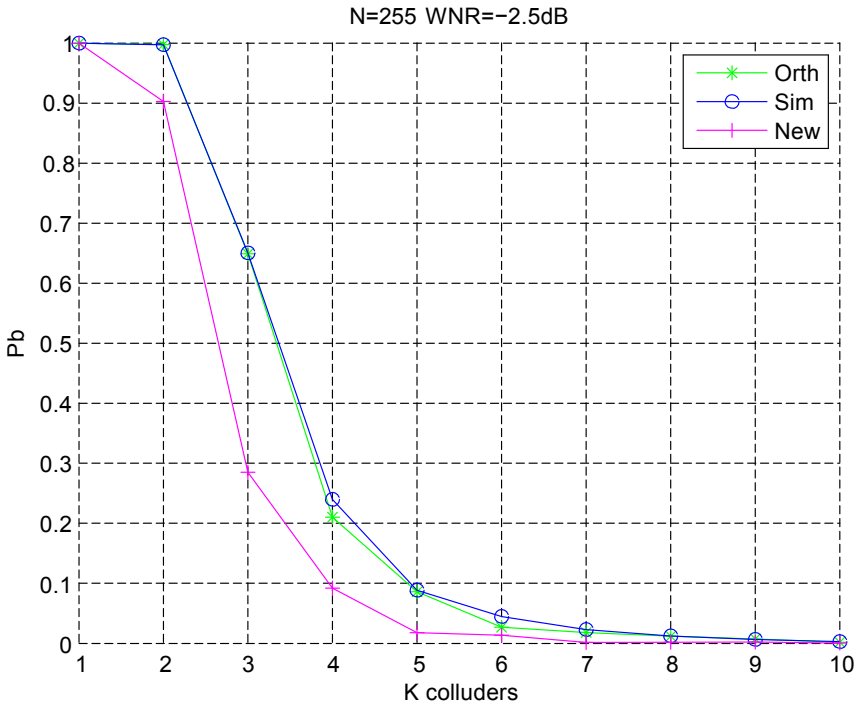


(e) WNR=5 dB

Figure 6.1: (a), (b), (c), (d), and (e) The probability of detecting at least one colluder P_d as a function of the number of colluders K, where $N = 63$ and WNR=-5 dB, WNR=-2.5 dB, WNR=0 dB, WNR=2.5 dB and WNR=5 dB respectively.

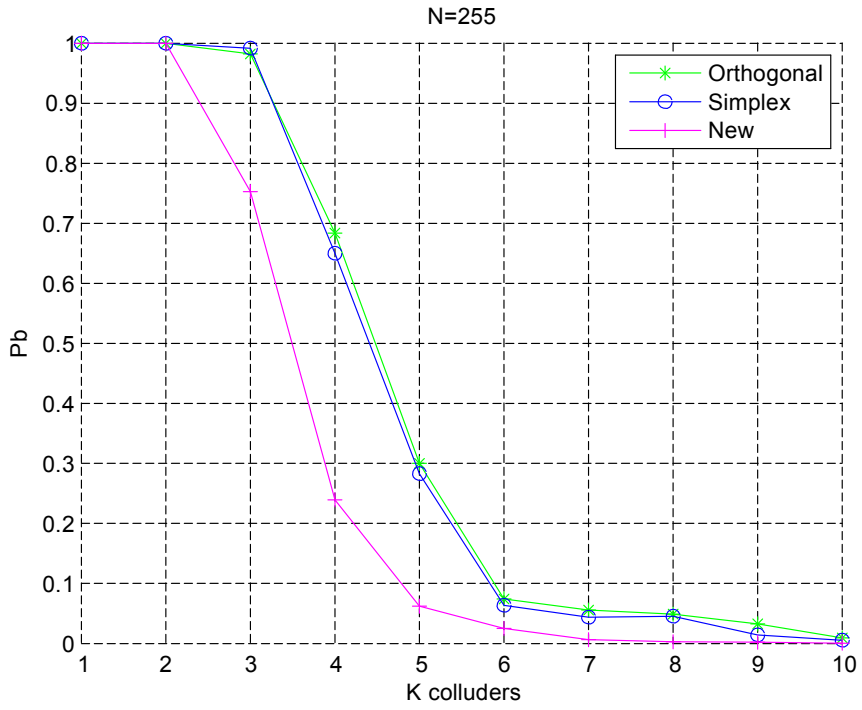


(a) WNR=-5 dB

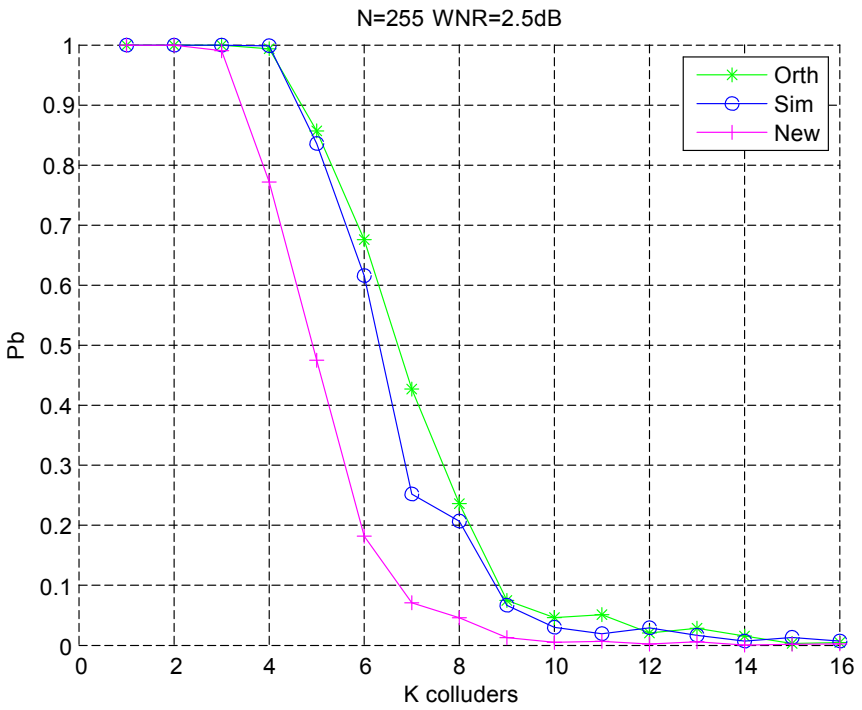


(b) WNR=-2.5 dB

Figure 6.2

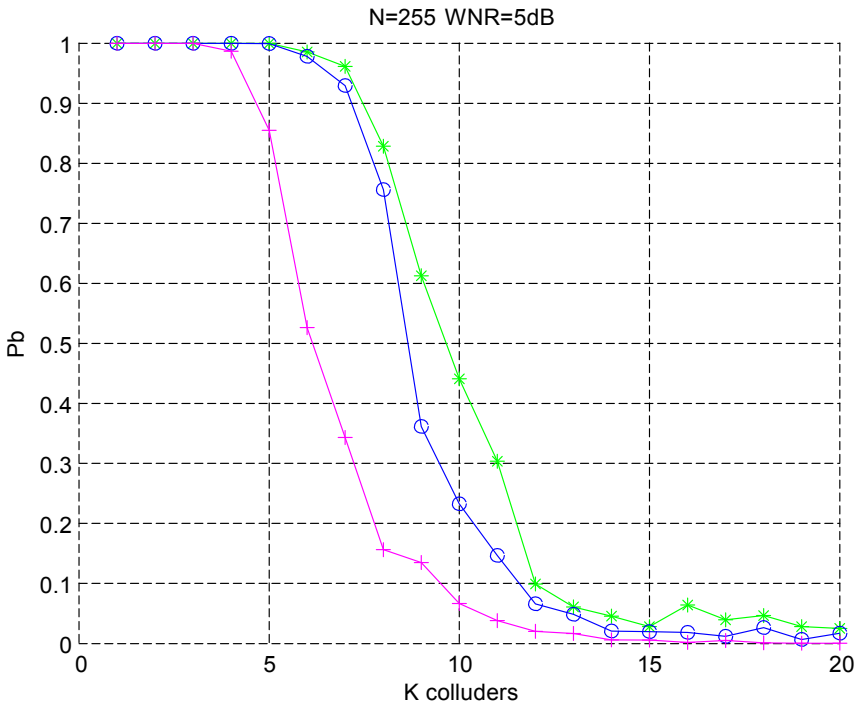


(c) WNR=0 dB



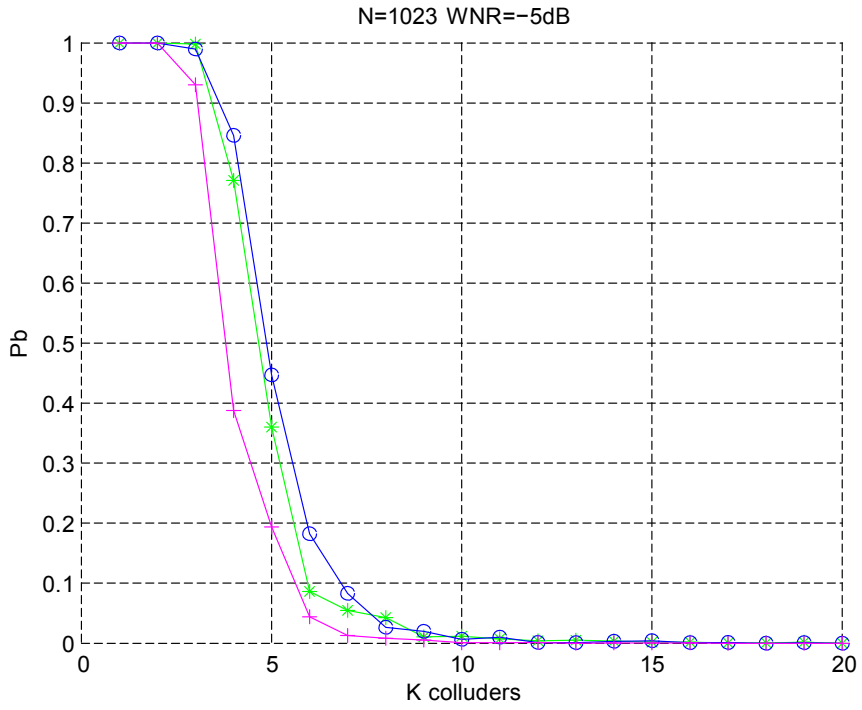
(d) WNR=2.5 dB

Figure 6.2

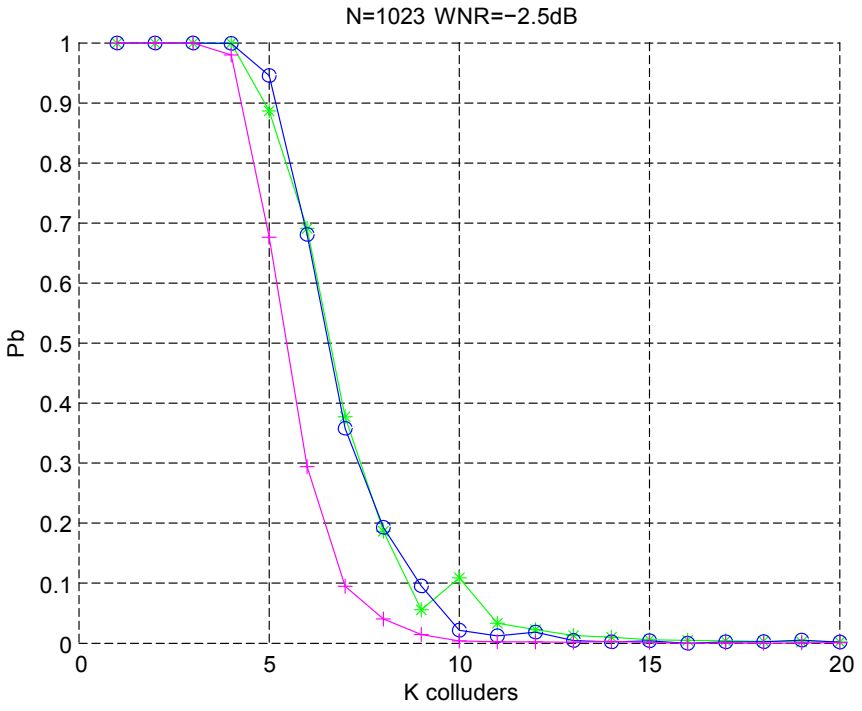


(e) WNR=5 dB

Figure 6.2: (a), (b), (c), (d), and (e) The probability of detecting at least one colluder P_d as a function of the number of colluders K, where $N = 255$ and WNR=-5 dB, WNR=-2.5 dB, WNR=0 dB, WNR=2.5 dB and WNR=5 dB respectively.

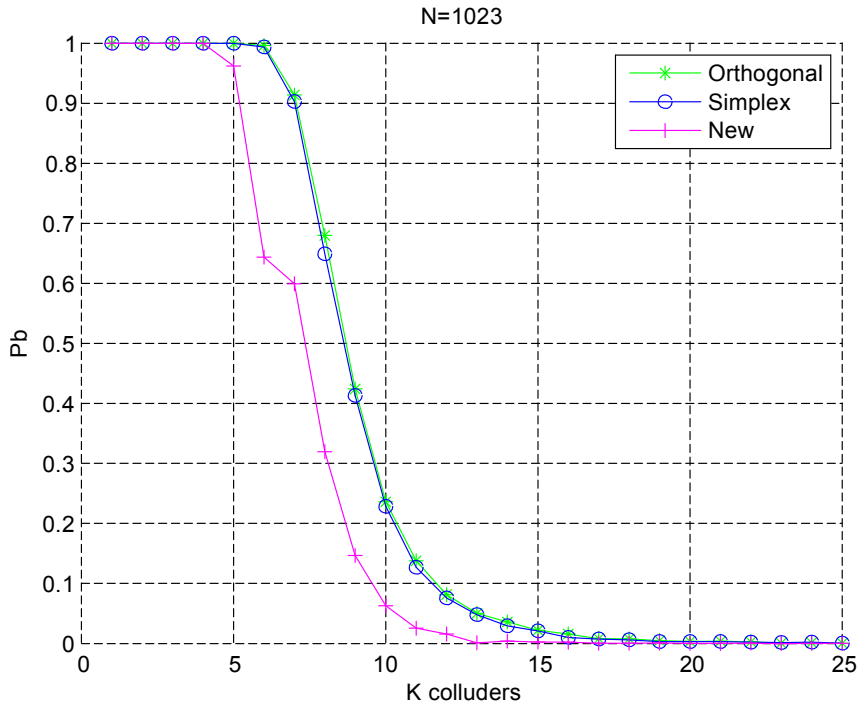


(a) WNR=-5 dB

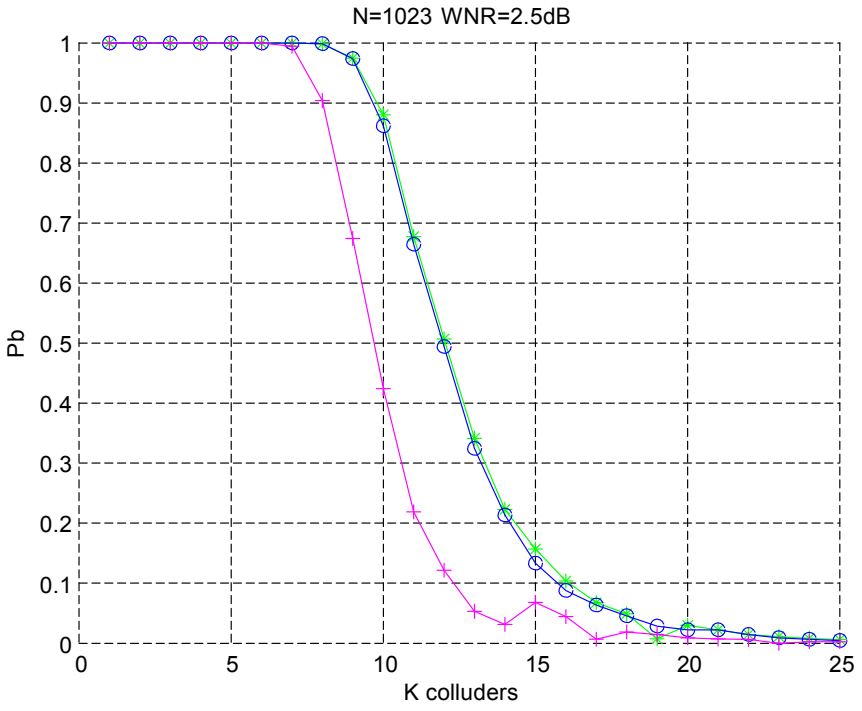


(b) WNR=-2.5 dB

Figure 6.3

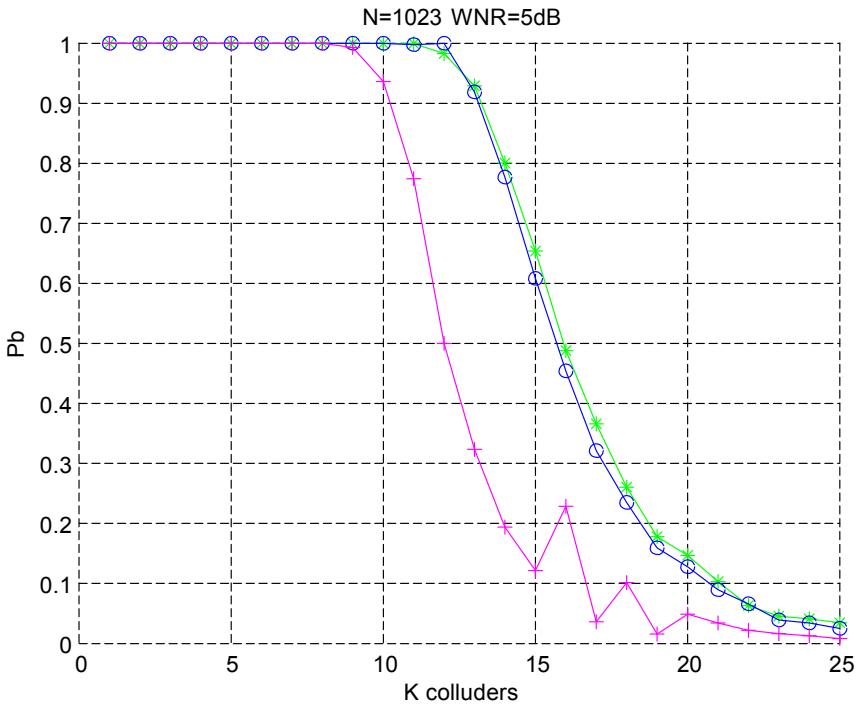


(c) WNR=0 dB



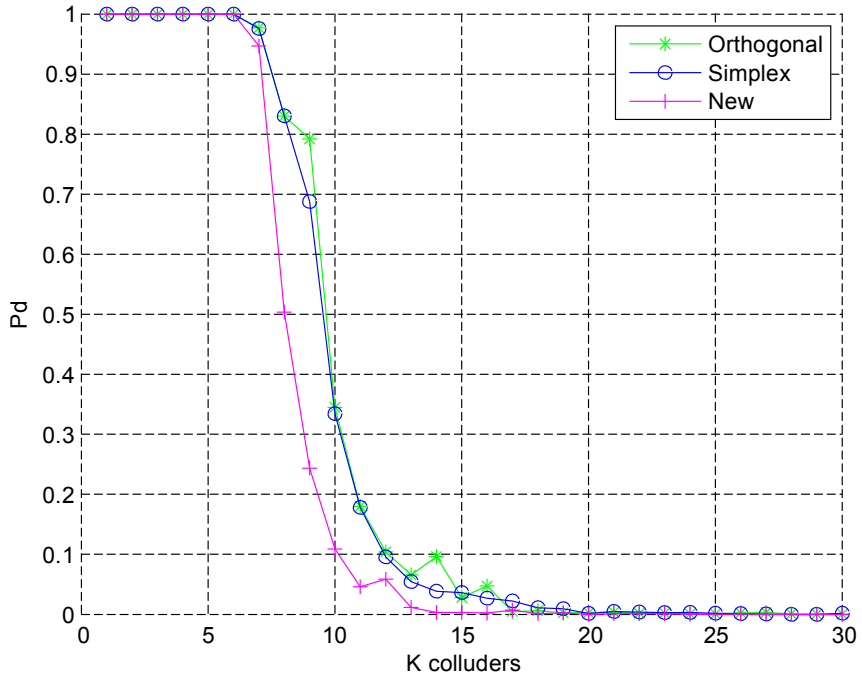
(d) WNR=2.5 dB

Figure 6.3

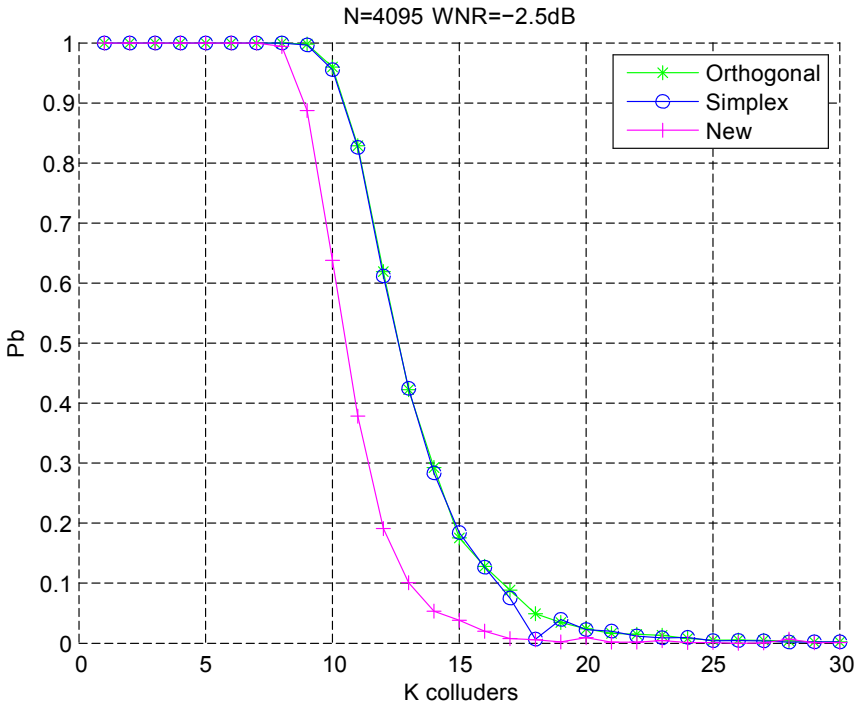


(e) WNR=5 dB

Figure 6.3: (a), (b), (c), (d), and (e) The probability of detecting at least one colluder P_d as a function of the number of colluders K, where $N = 1023$ and WNR=-5 dB, WNR=-2.5 dB, WNR=0 dB, WNR=2.5 dB and WNR=5 dB respectively.

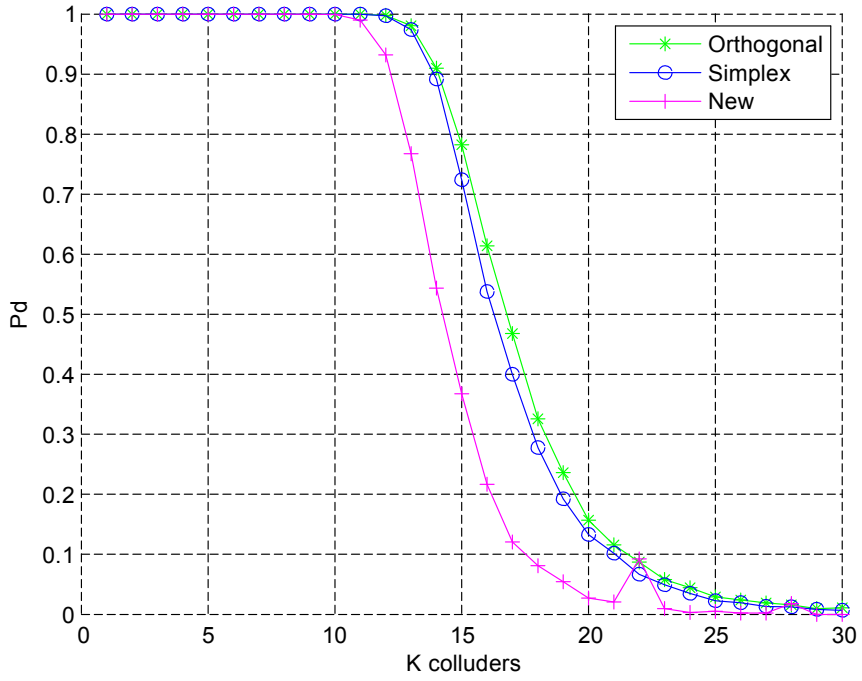


(a) WNR=-5 dB

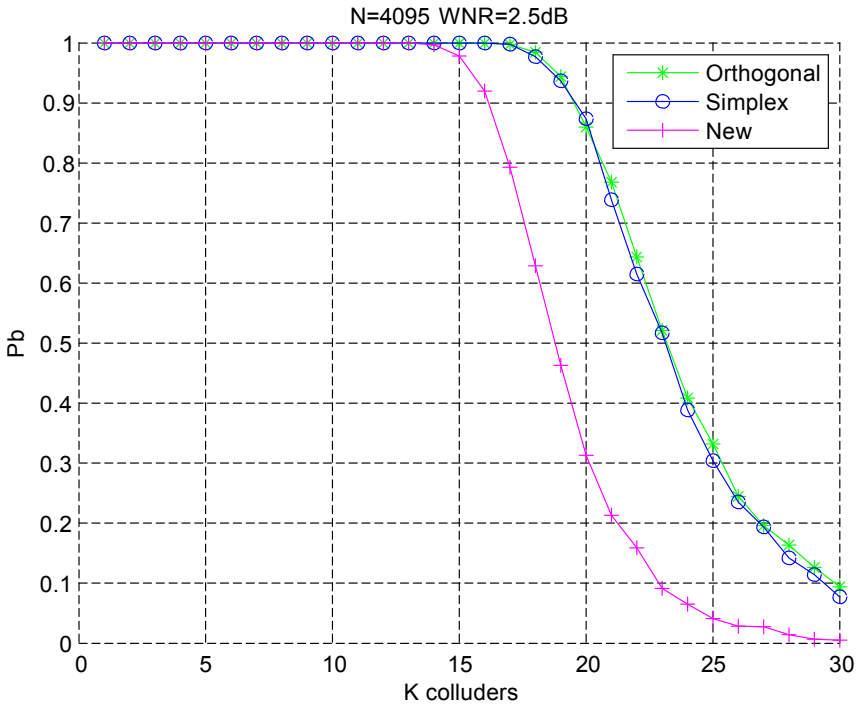


(b) WNR=-2.5 dB

Figure 6.4

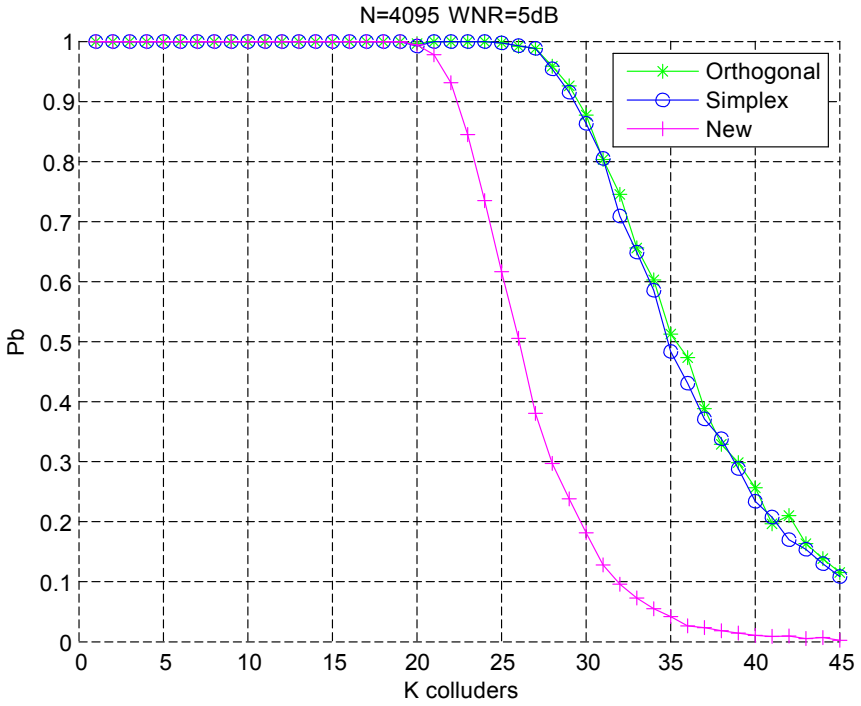


(c) WNR=0 dB



(d) WNR=2.5 dB

Figure 6.4



(e) WNR=5 dB

Figure 6.4: (a), (b), (c), (d), and (e) The probability of detecting at least one colluder P_d as a function of the number of colluders K, where $N = 4095$ and WNR=-5 dB, WNR=-2.5 dB, WNR=0 dB, WNR=2.5 dB and WNR=5 dB respectively.

Chapter 7

Conclusions

This thesis has presented a new fingerprint design using optical orthogonal codes. Compared to ETF fingerprints, our new fingerprint design has a more flexible structure which offers more parameters and less storage. In practice, we can achieve fast processing in detection using IFHT, which improves the speed of detection. Our new fingerprint system has a more flexible structure and can provide a faster detection process.

About the performance of our new fingerprint system, there are many more directions that need to be further investigated.

1) In the thesis, we assume that the attack model is average linear attack model when we compare the performances of fingerprint systems. Other types of attacks, minimum attack model, maximum attack model, median attack model, minmax attack model, modified negative attack model and random negative attack model are also very common for colluding multimedia data. It is necessary to study the gap of performances between our new fingerprints and the other two fingerprints under other attack models.

2) The relationship between the number of accommodated users and the maximum number of colluders that can be tolerated by systems needs to be investigated. The results of such an investigation will help us better understand the characteristic of one fingerprint system.

3) The threshold τ is an important factor that influences the performance of fingerprint systems. The smaller τ guarantees a high probability of catching colluders but increases the probability of accusing innocent users. How to choose a threshold to achieve the best performance can be further studied.

Bibliography

[1] D. Boneh and J. Shaw, "Collusion secure fingerprinting for digital data," *IEEE Trans. Information Theory*, 44(5): 1897-1905, Sept. 1998.

[2] H. Stone, "Analysis of attacks on image watermarks with randomized coefficients," *Technical Report 96-045, NEC Research Institute*, 1996.

[3] F. Ergun, J. Killian and R. Kumar, "A note on the limits of collusion-resistant watermarks," *Advances in Cryptology: Lecture Notes in Computer Science*, 1592: 140-149, 2001.

[4] J. Killian, T. Leighton, L. R. Matheson, T. G. Shamoon, R. Tajan and F. Zane, "Resistance of digital watermarks to collusive attacks," *Technical Report TR-585-98, Department of Computer Science, Princeton Univ.*, 1998.

[5] Z. J. Wang, M. Wu, H. Zhao, W. Trappe and K. J. R. Liu, "Collusion resistance of multimedia fingerprinting using orthogonal modulation," *In IEEE Trans. on Image Processing*, pp. 804-821, 2005.

[6] B. Chor, A. Fiat and M. Manor, "Tracing traitors," *IEEE Trans. Information Theory*, 46(3): 893-910, May 2000.

[7] G. Tardos, "Optimal probabilistic fingerprint codes," *J. ACM*, vol. 55, no. 2, p. 10, 2008.

[8] H. Chu, L. Qiao and K. Nahrstedt, "A secure multicast protocol with copyright protection," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 32, no. 2, pp. 42-60, Apr. 2002.

[9] B. Pfitzmann and M. Waidner, "Anonymous fingerprinting," *IBM Re-search*, Res. Rep. RZ 2881, 1996.

[10] B. Pfitzmann and M. Waidner, "Asymmetric fingerprinting for larger collusions," *in Proc. 4th ACM Conf. Computer and Communications Security,* pp. 151-160, 1997.

[11] S. Lin, M. Shahmohammadi and H. El Gamal, "Fingerprinting with minimum distance decoding, " *IEEE Trans. Inf. Forens. Security,* vol.4, no. 1, pp. 59-69, Mar. 2009.

[12] A. Somekh-Baruch and N. Merhav, "On the capacity game of private fingerprinting systems under collusion attacks," *IEEE Trans. Inf. Theory,* vol. 51, no. 3, pp. 884-899, Mar. 2005.

[13] A. Somekh-Baruch and N. Merhav, "Achievable error exponents for the private fingerprinting game," *IEEE Trans. Inf. Theory,* vol. 53, no. 5, pp. 1827-1838, May 2007.

[14] N. Anthapadmanabhan, A. Barg and I. Dumer, "On the fingerprinting capacity under the marking assumption," *IEEE Trans. Inf. Theory,* vol. 54, no. 6, pp. 2678-2689, Jun. 2008.

[15] A. Barg, G. R. Blakley, and G. A. Kabatiansky, "Digital fingerprinting codes: problem statements, constructions, identification of traitors," *IEEE Tran. on Inf. Theory,* vol. 49, no. 4, pp. 852-865, April 2003.

[16] M. Cheng and Y. Miao, "On anti-collusion codes and detection algorithms for multimedia fingerprinting," *IEEE Trans. Inf. Theory,* vol. 57, no. 7, pp. 4843-4851, Jul. 2011.

[17] J. Cotrina-Navau and M. Fernndez, "A family of asymptotically good binary fingerprinting codes," *IEEE Trans. Inf. Theory,* vol. 56, no. 10, pp. 5335-5343, Oct. 2010.

[18] D. Boneh, A. Kiayias and H. Montgomery, "Robust fingerprinting codes: A near optimal construction," *in Proc. 10th Annu. ACM Work-shop Dig. Rights Manag.,* pp. 3-12, 2010.

[19] H. Koga and Y. Minami, "A digital fingerprinting code based on a projective plane and its identifiability of all malicious users," *IEICE Trans. Fund. Electron., Commun. Comput. Sci.,* vol. 94, no. 1, pp. 223-232, 2011.

[20] W. Trappe, M. Wu, Z. Wang and K. Liu, "Anti-collusion fingerprinting for multimedia," *IEEE Trans. Signal Process.,* vol. 51, no. 4, pp. 1069-1087, Apr. 2003.

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

[22] **J.** Kilian, F. Leighton, L. Matheson, T. Shamoon, R. Tarjan and F.Zane, "Resistance of digital watermarks to collusive attacks," *In Proc. IEEE Int. Symp. Inf. Theory,* p. 271, 1998.

[23] F. Ergun, **J.** Kilian and R. Kumar, "A note on the limits of collusion-resistant watermarks," *In Proc. Adv. Cryptol. EUROCRYPT,* pp. 140-149, 1998.

[24] T. Wu and S. Wu, "Selective encryption and watermarking of mpeg video," *Proc.Int. Conf. on Imaging Science, Systems, and Technology,* June 1997.

[25] Z. Wang, M. Wu, H. Zhao, W. Trappe and K. Liu, "Anti-collusion forensics of multimedia fingerprinting using orthogonal modulation," *IEEE Trans. Image Process.,* vol. 14, no. 6, pp. 804-821, Jun. 2005.

[26] N. Kiyavash, P. Moulin and T. Kalker, "Regular simplex fingerprints and their optimality properties," *IEEE Trans. Inf. Forens. Security,* vol.4, no. 3, pp. 318-329, Sep. 2009.

[27] M. Fickus, D. G. Mixon, C. J. Quinn and N. Kiyavash, "Fingerprinting with equiangular tight frames," *IEEE Trans. Inf.*, vol. 59, No. 3, pp. 1855-1865, 2013.

[28] M. Fickus, D. G. Mixon and **J.** Tremain, "Steiner equiangular tight frames," *Linear Algebra Appl.*, vol. 436, no. 5, pp. 1014-1027, 2012.

[29] A. Piva, F. Bartolini and M. Barni, "Managing, copyright in open networks," *IEEE Internet Computing,* pp. 18-26, May/June 2002.

[30] W. Trappe, M. Wu, Z. **J.** Wang and K. **J.** R. Liu, "Anti-collusion fingerprinting for multimedia," *IEEE Trans. on Signal Processing,* 51(4): 1069-1087, April 2003.

[31] B. Thomas, **J.** Dieter and L. Hanfried, *Design Theory Cambridge,* Cambridge University Press., 2nd ED, pp. 20-68, 1999.

[32] E.F. Assmus and J.D. Key, *Designs and Their Codes*, Cambridge University Press., pp. 90-120, 1992.

[33] F. R. K. Chung, J. A. Salehi and V. K. Wei, "Optical orthogonal codes: Design, analysis, and applications," *IEEE Trans. Inf. Theory,* vol. IT-35, pp. 595-604, May 1989.

[34] N. Y. Yu and N. Zhao, "Deterministic construction of real-valued ternary sensing matrices using optical orthogonal codes," *IEEE Signal Processing Letters,* vol. 20, no. 11, pp 1106-1109, Nov. 2013.

[35] R. C. Bose and S. Chowla, "Theorems in the additive theory of numbers," *Mathematical Sciences Directorate,* pp. 141-147, 1963.

[36] B. J. Fino and V. R. Algazi, "Unified matrix treatment of the fast WalshHadamard transform," *IEEE Trans. Computers*, pp. 1142-1146, Nov. 1976.

[37] J. Munkres, *Elements of Algebraic Topology,* Addison-Wesley Reading, 2nd, May. 1984.

[38] J. Singer, "A theorem in finite projective geometry and some applications to number theory," *Trans. Amer. Math. Soc.,* vol. 43, pp. 377-385, 1938.

[39] I. Z. Rusza, "Solving a linear equation in a set of integers I," *Acta Aritmetica,* pp. 259-282, 1993.

[40] B. Lindström, "An inequality for B2-sequences," *Journ, Combin. Theory,* vol. 6, pp. 211-212, 1996.

[41] M. Wu, W. Trappe, Z. J. Wang and K.J. Ray Lin, "Conclusion resistance fingerprinting for multimedia," *IEEE Signal Proc.* vol. 4, pp. 15-27, Mar. 2004.

[42] H. Zhao, "Multimedia fingerprinting for multiuser forensics and security," *University of Maryland,* Doctor Thesis, pp. 1-196, 2004.

[43] C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs,* 2nd ed. London, U.K.: Chapman & Hall/CRC, pp. 1-55, 2007.

[44] H. O. Kunz, "On the equivalence between one dimensional discrete Walsh-Hadamard and multidimensional discrete Fourier transforms," *IEEE Tran. on Computer*, vol. 28, no. 3, pp. 267-268, Mar. 1979.

[45] N. Kiyavash and P. Moulin, "Sphere packing lower bound on fingerprinting error probability," in *Proceedings of SPIE*, vol. 6505, 2007.