Design of New Fingerprinting Codes Using Optical Orthogonal Codes

Na Zhao
Department of Physics
Ryerson University
Toronto, Ontario, Canada
Email: zhaona05012007@hotmail.com

Nam Yul Yu
School of Information and Communications
Gwangju Institute of
Science and Technology (GIST)
Gwangju, Korea
Email: nyyu@gist.ac.kr

***Abstract*—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 collude to create a forged copy by combining their ones. The collusion is modeled as a linear averaging attack, where multiple weighted copies are averaged and the Gaussian noise is then added to the averaged copy. In this paper, a new fingerprint design robust to collusion is proposed, which is to accommodate a lot more users 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 will be used as a fingerprint. The focused detection is used to determine whether a user is innocent or guilty in a collusion of linear averaging attack. Simulation results show that the performance of our new fingerprint design is comparable to that of orthogonal and simplex fingerprints.**

***Keywords*—digital fingerprints, fast Hadamard transform, modular Golomb rulers, optical orthogonal codes (OOC)**

I. Introduction

Digital fingerprint technology is one important branch of information hiding for copyright protection. It is an effective technique to make 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 becomes a threat which will deter the users to release unauthorized copies. However, multiple users can collude to identify or distort a fingerprinted copy and make the content owner difficult to detect distributors.

There are two approaches in design of fingerprints robust to such a collusion: *marking assumption* and *distortion assumption*. In this paper, we consider distortion assumption only, and readers are referred to [1] for marking assumption. In distortion assumption regime, a unique fingerprint introduces a noise-like distortion to digital media. The power of the fingerprint should be perceptually invisible, which aims to ensure the quality of original media. In terms of distortion assumption, a fingerprinting technology involves an embedding process. Watermarking relevant to fingerprinting is a well known technology in this regime. Cox *et al.* [2] proposed a secure algorithm by inserting a watermark constructed as an independent and identically distributed (i.i.d) Gaussian random vector. The insertion guarantees the overall quality of the media and makes the colluders difficult to remove the watermark. More efforts of watermarking can be found in [3] and [4]. Wang *et al.* [5] proposed a specific fingerprint design using Gaussian distributed fingerprints and orthogonal modulation. They considered an averaging collusion attack to analyze the robustness of the designed fingerprint system. Kiyavash, Moulin and Kalker [6] proposed an optimal structure of n simplex fingerprints in terms of maximizing the error exponent of the detection test. Recently, Mixon, Quinn, Kiyavash and Fickus [7] designed a fingerprint system using equiangular tight frames (ETF) [8], where the Steiner system [9] has been exploited to construct the ETF. The performance of the ETF fingerprints is comparable to that of orthogonal and simplex fingerprints, but they can accommodate more users.

In this paper, we present a new fingerprint design using *optical orthogonal codes (OOC)* under distortion assumption. In the construction, each cyclic shift of binary sequences in an OOC is arranged as each column of a base matrix. Then, the 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 fingerprint is motivated by the Steiner ETF fingerprint [7], but it offers a more flexible structure. Our fingerprint scheme just needs to remember a few binary sequences instead of the full base matrix, which requires less storage space in practical implementation. Moreover, our new fingerprints can provide more parameters for fingerprint lengths than the ETF fingerprints. Similar to the ETF fingerprints, our new fingerprints can accommodate a lot more users than orthogonal and simplex fingerprints. Finally, the fast Hadamard transform technique can be employed to improve the speed of construction and detection processes.

This paper is organized as follows. Section II introduces a mathematical formulation of a fingerprint system. Section III then presents the new fingerprint construction using optical orthogonal codes and makes the error analysis. In Section IV, the detection process of our new fingerprints will be discussed using the fast Hadamard transform technique. In Section V, we will give the results of simulations and demonstrate the performance of our new fingerprint design. Concluding remarks will be given in Section VI.

This work was supported by the NSERC of Canada. The work of the second author was also supported by the Global University Project (GUP) of GIST, Korea.

II. Mathematical Formulation

This section reviews a mathematical model of [7] to describe fingerprint scheme, attack model, and detection process.

A. Fingerprinting and attack model

A host signal is modeled as $\mathbf{s} = (s_0, s_1, \cdots, s_{N-1})^T$ where $s_i \in \mathbb{R}$, which will be given to M users. In order to deter illegal distribution, a content owner embeds the host signal with *fingerprints* before distribution. Precisely, the mth user's copy is

$$\mathbf{x}_m = \mathbf{s} + \mathbf{f}_m$$

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

$$\gamma^2 = ||\mathbf{f}_m||^2 = ND_f \tag{1}$$

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

Let $\mathcal{K} \subseteq \{0, \cdots, M-1\}$ denote a group of users who forge a copy of the host signal. Then, the *linear averaging attack* is of the form

$$\mathbf{y} = \sum_{k\in\mathcal{K}} \alpha_k(\mathbf{s} + \mathbf{f}_k) + \boldsymbol{\epsilon}, \qquad \sum_{k\in\mathcal{K}} \alpha_k = 1 \tag{2}$$

where $\boldsymbol{\epsilon}$ is a noise vector introduced by the colluders. In (2), α_k is the weight of the kth colluder's copy in the forgery, and $\boldsymbol{\alpha} = (\alpha_0, \cdots, \alpha_{M-1})$ is a vector of all the colluders' weights. Assume that $\boldsymbol{\epsilon}$ is a Gaussian noise vector with zero mean and variance $N\sigma^2$, 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

$$\mathrm{WNR} = 10\log_{10}\left(\frac{ND_f}{N\sigma^2}\right).$$

B. Detection

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

In focused detection, the host signal $\mathbf{s}$ is subtracted from the forgery of (2), which yields

$$\mathbf{z} = \mathbf{y} - \mathbf{s} = \sum_{k\in\mathcal{K}} \alpha_k \mathbf{f}_k + \boldsymbol{\epsilon}. \tag{3}$$

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

$$T_m(\mathbf{z}) = \frac{1}{\gamma^2}\langle \mathbf{z}, \mathbf{f}_m \rangle \tag{4}$$

where γ^2 is the fingerprint energy in (1).

For the mth user, let $H_1(m)$ denote the guilty hypothesis ($m \in \mathcal{K}$) and $H_0(m)$ the innocent hypothesis ($m \notin \mathcal{K}$). With a threshold τ, the detection rule is described by

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

The performance analysis of the focused detection will be explicitly discussed in Section III.

III. New Fingerprint Design

In this section, a new fingerprint design using optical orthogonal codes (OOC) is presented.

A. 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 [10] 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: [10] An (n, w, λ) *optical orthogonal code (OOC)* is a family of S binary sequences of period n, i.e., $\mathcal{F} = \{\mathbf{s}^{(i)} \mid 0 \leq i \leq S-1\}$. In the OOC family $\mathcal{F}$, each binary sequence has the constant Hamming weight w and the Hamming correlation satisfies $\theta_{\mathbf{s}^{(i)},\mathbf{s}^{(j)}} \leq \lambda$ for any (i, j) and for every τ, where $\tau \neq 0$ if $i = j$.

B. Modular Golomb rulers

Definition 2: [9] 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 $\{d_i - d_j \mid 0 \leq i \neq j \leq k-1\}$ 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

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

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 clearly 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 $S = 1$.

C. New fingerprints using OOCs

Our fingerprint design is motivated to remedy the potential drawbacks of the *Steiner ETF fingerprints* [7]. First of all, the indices of all nonzero entries of the base matrix need to be remembered in the Steiner ETF fingerprints, which requires large storage space when the signal dimension N and the number of users M are large in practice. Second, the base matrix from the Steiner system is extended by a Hadamard matrix, which imposes a restriction on the parameters to yield real-valued fingerprints. Due to the optimal structure of Steiner systems, the restriction allows relatively few parameters for N and M in the Steiner ETF fingerprints. More details on the drawbacks have been discussed in [11].

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, which is the main contribution of this paper. In what follows, we assume that the entries of the Hadamard matrix $\mathbf{H}$ are ± 1.

Construction 1: Let $\{\mathbf{s}^{(i)} \mid 0 \leq i \leq S-1\}$ 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 $\mathbf{B}$. Then, the support of the tth column of $\mathbf{B}$ is given by

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

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 $\nu = w + \delta$ such that $\nu \equiv 0 \pmod 4$. Then use a $\nu \times \nu$ 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 ν. The extension yields an $n \times \nu L$ matrix $\mathbf{B}_e = [\mathbf{B}_{e,0}|\cdots|\mathbf{B}_{e,L-1}]$, where $\mathbf{B}_{e,j}$ denotes an $n \times \nu$ submatrix extended from a single column of $\mathbf{B}$ for $0 \le j \le L-1$.

3) A new fingerprints system is given by $\mathbf{F} = \frac{1}{\sqrt{w}}\mathbf{B}_e = [\mathbf{F}_0|\cdots|\mathbf{F}_{L-1}]$, where $\mathbf{F}_j = \frac{1}{\sqrt{w}}\mathbf{B}_{e,j}$ for $0 \le j \le L-1$. Each column of $\mathbf{F}$ is used as each user's fingerprint, which has the entries of 0 and $\pm\frac{1}{\sqrt{w}}$. The length of each fingerprint is $N = n$ and the total number of available fingerprints is $M = \nu nS$.

In fact, Construction 1 was originally presented in [11] for compressed sensing matrices. It is now applied in new fingerprint design for low coherence of distinct fingerprints. In Construction 1, the *coherence* of $\mathbf{F} = \{\mathbf{f}_m\}_{m=0}^{M-1}$ is defined as the maximum magnitude of inner products between a pair of distinct fingerprints, i.e., $\mu = \max_{i \ne j}\langle \mathbf{f}_i, \mathbf{f}_j \rangle$. The coherence of $\mathbf{F}$ is given by [11]

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

Particularly, if $w = O(\sqrt{n})$ for small λ, $\delta = O(1)$, the fingerprints system $\mathbf{F}$ has the coherence of $O(\frac{1}{\sqrt{N}})$. The coherence of our new fingerprints system is sufficiently low, but not optimal. However, simulation results demonstrate that it has slight performance degradation, compared to orthogonal and simplex fingerprints systems with optimal structure, while having much more fingerprints available.

In what follows, we present a construction example of OOCs by employing the modular Golomb rulers obtained from the Bose-Chowla construction [12]. Then we use the resulting OOCs to construct new fingerprints. The following definition of the Bose-Chowla construction is from [13].

Definition 3: [13] Let $q = p^m$ for prime p and a positive integer m. Let β be a primitive element in a finite field $\mathrm{GF}(q^2)$. Define

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

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 3. Then $\mathcal{F} = \{\mathbf{s}\}$ is an $(n, w, 1)$ OOC of family size $S = 1$, where $n = q^2 - 1$ and $w = q$. Set $\nu = w + \delta \equiv 0 \pmod 4$ for small δ, $0 \le \delta < w$. With the OOC and a $\nu \times \nu$ Hadamard matrix, Construction 1 gives an $N \times M$ fingerprints system, where $N = q^2 - 1$ and $M = \nu N$. In particular, if $q = 2^m$ and $\delta = 0$, our new fingerprints system has $N = 2^{2m} - 1$, $M = 2^m(2^{2m}-1)$, and $\mu \le \frac{1}{2^m}$.

D. Error analysis for new fingerprint design

In what follows, our new fingerprints of Constructions 1 and 1.1 are examined by the error probabilities in detection process, where we use the analysis technique made in [7]. The error analysis then yields almost the same results as those of [7], replacing the coherence parameter by that of our new fingerprints.

We analyze two types of errors for detection process, *false positive* (type I) and *false negative* errors (type II). The former is the probability $P_{\mathrm{I}}(\mathbf{F}, m, \tau, \mathcal{K}, \boldsymbol{\alpha})$ that an innocent user m ($\notin \mathcal{K}$) is found guilty ($T_m(z) \ge \tau$), which should be kept extremely low. The latter is the probability $P_{\mathrm{II}}(\mathbf{F}, m, \tau, \mathcal{K}, \boldsymbol{\alpha})$ that a guilty user m ($\in \mathcal{K}$) is found innocent ($T_m(z) < \tau$). The error probabilities depend on the fingerprints $\mathbf{F}$, the coalition $\mathcal{K}$, the weight vector $\boldsymbol{\alpha}$, and the threshold τ. The formulations of error analysis in [7] are summarized in Table I.

In Table I, $P_{\mathrm{I}}(\mathbf{F}, \tau, \boldsymbol{\alpha})$ and $P_{\mathrm{II}}(\mathbf{F}, \tau, \boldsymbol{\alpha})$ are the worst case probabilities of type I and type II errors, respectively. Moreover, the maximum of these two error probabilities is defined as the *worst case* error probability of

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

By changing the threshold parameter τ to minimize the worst case error probability, the *minmax* error probability is defined as

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

Theorem 1 analyzes the worst case probabilities of type I and type II errors, and then develops the bounds of the minmax error probability. The proof of Theorem 1 is omitted here, since it is similar to those of Theorems 7 and 8 in [7].

Theorem 1: Recall γ, D_f and σ in Section II. Consider our new fingerprints system $\mathbf{F} = \{\mathbf{f}_m\}_{m=0}^{M-1}$, where each fingerprint has the length of N. Then, the worst case probabilities of type I and type II errors satisfy

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

The minmax error probability can be bounded as

$$Q\left(\frac{d^*_{\mathrm{low}}}{2}\right) \le P_{\mathrm{minmax}}(\mathbf{F}, \boldsymbol{\alpha}) \le Q\left(\frac{d^*_{\mathrm{up}}}{2}\right)$$

where

$$d^*_{\mathrm{low}} = \frac{\sqrt{\frac{M}{M-1}}\sqrt{ND_f}}{\sigma\sqrt{K(K-1)}},$$
$$d^*_{\mathrm{up}} = \frac{\sqrt{ND_f}}{\sigma K}\left(1 - (2K-1)\mu'\right)$$

TABLE I. FORMULATIONS OF ERROR ANALYSIS

False positive error	False negative error
$P_{\rm I}(\mathbf{F}, m, \tau, \mathcal{K}, \boldsymbol{\alpha}) = \text{Prob}[T_m(z) \geq \tau \mid H_0(m)]$	$P_{\rm II}(\mathbf{F}, m, \tau, \mathcal{K}, \boldsymbol{\alpha}) = \text{Prob}[T_m(z) < \tau \mid H_1(m)]$
$P_{\rm fa}(\mathbf{F}, \tau, \mathcal{K}, \boldsymbol{\alpha}) = \max_{m \notin \mathcal{K}} P_{\rm I}(\mathbf{F}, m, \tau, \mathcal{K}, \boldsymbol{\alpha})$	$P_{\rm md}(\mathbf{F}, \tau, \mathcal{K}, \boldsymbol{\alpha}) = \min_{m \in \mathcal{K}} P_{\rm II}(\mathbf{F}, m, \tau, \mathcal{K}, \boldsymbol{\alpha})$
$P_{\rm I}(\mathbf{F}, \tau, \boldsymbol{\alpha}) = \max_{\mathcal{K}} P_{\rm fa}(\mathbf{F}, \tau, \mathcal{K}, \boldsymbol{\alpha})$	$P_{\rm II}(\mathbf{F}, \tau, \boldsymbol{\alpha}) = \max_{\mathcal{K}} P_{\rm md}(\mathbf{F}, \tau, \mathcal{K}, \boldsymbol{\alpha})$
–	$P_{\rm d}(\mathbf{F}, \tau, \mathcal{K}, \boldsymbol{\alpha}) = 1 - P_{\rm md}(\mathbf{F}, \tau, \mathcal{K}, \boldsymbol{\alpha})$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{u^2}{2}} du$ and K is the number of colluders. In the above bounds, $\mu' = \max\left(\frac{\lambda}{w}, \frac{\delta}{w}\right)$ for Construction 1, whereas $\mu' = \frac{1}{q}$ for Construction 1.1.

IV. FAST PROCESSING IN DETECTION

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

In Construction 1.1, the fingerprints system is presented as a matrix $\mathbf{F} = \{\mathbf{f}_m\}_{m=0}^{M-1} = [\mathbf{f}_0 \mid \mathbf{f}_1 \mid \cdots | \mathbf{f}_{M-1}]$, where each column $\mathbf{f}_i$ represents the ith user's fingerprint for $0 \leq i \leq M-1$. The length of the fingerprint is N, and M users are accommodated in total. In Construction 1, recall that the support of the first column of the base matrix is $\mathbf{d}^{(0)} = \{d_0^{(0)}, \cdots, d_{w-1}^{(0)}\}$, which yields the support of the kth column of the base matrix as

$$\mathbf{d}^{(k)} = \{d_h^{(0)} - k \pmod N \mid h = 0, 1, \cdots, w-1\} \quad (5)$$

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

In the fingerprints $\mathbf{F}$, let us define an $N \times \nu$ subsystem $\mathbf{F}_k = [\mathbf{f}_{k\nu} \mid \cdots \mid \mathbf{f}_{(k+1)\nu-1}]$ from which $\mathbf{F} = [\mathbf{F}_0 \mid \cdots \mid \mathbf{F}_{N-1}]$. Then, the fingerprints of $\mathbf{F}_k$ share the same support $\mathbf{d}^{(k)}$ in (5) as they are from a common sequence. Moreover, all the nonzero entries of $\mathbf{F}_k$ form a $w \times \nu$ matrix $\frac{1}{\sqrt{w}}\widetilde{\mathbf{H}} = \frac{1}{\sqrt{w}}[\mathbf{h}_0 \mid \cdots \mid \mathbf{h}_{\nu-1}]$, where $\mathbf{h}_i$ is the ith column of $\widetilde{\mathbf{H}}$, $0 \leq i \leq \nu - 1$. Clearly, each row of $\widetilde{\mathbf{H}}$ is from a $\nu \times \nu$ Hadamard matrix.

In detection process, let $t_{k\nu+j}$ be the $(k\nu + j)$th user's test statistic, where $0 \leq j \leq \nu - 1$. From (4), $t_{k\nu+j}$ is the normalized inner product of the fingerprint $\mathbf{f}_{k\nu+j}$ and $\mathbf{z}$ in (3). In order to reduce the computational complexity, extracting the nonzero entries from $\mathbf{f}_{k\nu+j}$ allows to write $t_{k\nu+j}$ as

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

where $\mathbf{z}_{\mathbf{d}^{(k)}}$ is a $w \times 1$ vector that takes only w entries out of $\mathbf{z}$ from the indices of the support $\mathbf{d}^{(k)}$. Finally, a $\nu \times 1$ vector $\mathbf{t}_k = [t_{k\nu}, \cdots, t_{(k+1)\nu-1}]^T$, a set of test statistics of ν users having their fingerprints $\{\mathbf{f}_{k\nu}, \cdots, \mathbf{f}_{(k+1)\nu-1}\}$, can be computed as

$$\mathbf{t}_k = \frac{1}{\gamma^2\sqrt{w}} \widetilde{\mathbf{H}}^T \mathbf{z}_{\mathbf{d}^{(k)}}. \quad (6)$$

In (6), the matrix-vector multiplication has the computational complexity of $O(\nu^2)$. Since $\widetilde{\mathbf{H}}$ is a partial Hadamard matrix, one can employ the fast Hadamard transform technique [14] for (6), which will reduce the complexity to $O(\nu \log_2 \nu)$. Therefore, the computational complexity of all the users' test statistics turns out to be $O(\nu N \log_2 \nu)$, or $O(M \log_2 \nu)$. In practice, the fast processing technique improves the speed of detection and construction.

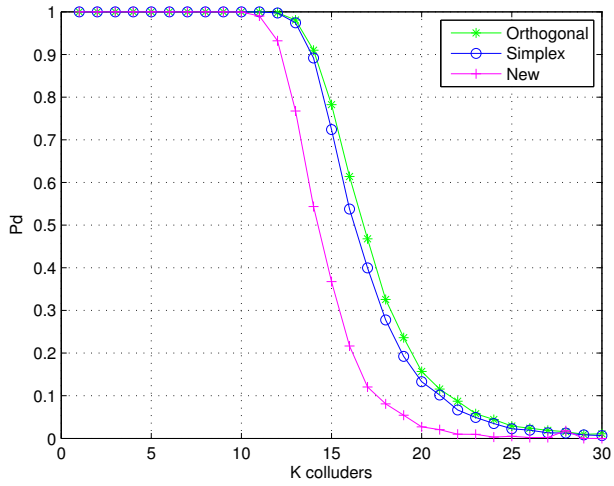
V. SIMULATION RESULTS

In order to measure the robustness of various fingerprint systems, we compare the maximum number of colluders which can be tolerated. The probability of detecting at least one colluder, denoted as $P_{\rm d}$, will be plotted as a function of the number of colluders K. In detection process, the threshold τ is chosen to guarantee reasonably low $P_{\rm fa}$. We assume that a fingerprint system requires $P_{\rm d} \geq 0.8$ and $P_{\rm fa} \leq 10^{-3}$ [5], since higher $P_{\rm d}$ and lower $P_{\rm fa}$ are necessary to guarantee the robustness of the system.

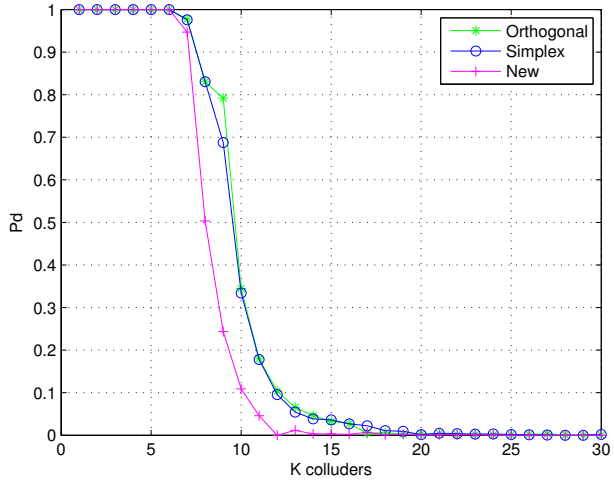
In this section, we compare the performance of orthogonal, simplex and new fingerprint systems for $N = 4095$. The orthogonal fingerprints have each column of an identity matrix as each user's fingerprint, where the total number of users equals to $M = N$. We use simplex fingerprints having the same power (γ) and the same inner product ($-\frac{1}{N}$) [13], where $M = N+1$. Our fingerprints are from Construction 1.1, where $q = 64$, $\delta = 0$, $\nu = q$, and $M = \nu N$. While orthogonal and simplex fingerprints accommodate 4095 and 4096 users, respectively, our fingerprints can support much more users up to $262,080$ – about 64 times more. Due to technical difficulties in simulation, only $32,768$ fingerprints have been simulated.

In experiments, total 3000 averaging attacks were simulated for each fingerprint system and collusion size K. Colluders were chosen randomly, and their copies were uniformly averaged to form a forgery. The Gaussian noise with power σ^2 per dimension was added to the forged copy. A threshold τ was chosen to ensure $P_{\rm fa} \leq 10^{-3}$. For each attack, $P_{\rm d}$ was measured by detecting every user in the fingerprint system.

Figure 1 displays $P_{\rm d}$ as a function of collusion size K for orthogonal, simplex and our new fingerprints, where WNR is 0 dB and -5 dB, respectively. Clearly, $P_{\rm d}$ approaches 0 as the number of colluders increases. The maximum numbers of colluders that can be tolerated by orthogonal and simplex fingerprint systems are similar to each other, and approximately one or two more users are tolerated than in our new fingerprint system. Overall, our new fingerprints system accommodates a lot more users at the cost of slightly worse detection performance, compared to orthogonal and simplex fingerprints. Figure 1 (a) and (b) show that the performance gap between our new fingerprints and the other two gets tighter as the noise level increases. We have also examined the performance for $N = \{63, 255, 1023\}$, where we observed the similar trend.



(a) WNR = 0 dB



(b) WNR = -5 dB

Fig. 1. The probability of detecting at least one colluder P_d as a function of the number of colluders K, where $N = 4095$ and WNR = 0 dB and -5 dB, respectively.

In summary, simulation results showed that our new fingerprints system could support a huge number of users, about 64 times more than conventional systems, at the cost of slight performance degradation. Therefore, the new fingerprints system looks favorable to accommodate a large number of users in case a small number of potential colluders exist in noisy environment.

VI. Conclusions

This paper has presented a new fingerprint design using optical orthogonal codes. Compared to ETF fingerprints, our new fingerprint design offers flexible structure which provides more parameters and requires less storage. Also, our new fingerprints system accommodates much more users than orthogonal and simplex fingerprints, at the cost of slight performance degradation. In practice, fast detection processing with low complexity can be achieved by means of the fast Hadamard transform technique.

References

[1] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inf. Theory,* vol. 44, no. 5, pp. 1897-1905, Sep. 1998.

[2] 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.

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

[4] F. Ergun, J. Kilian, and R. Kumar, "A note on the limits of collusion-resistant watermarks," *In Proc. Adv. Cryptol. - EUROCRYPT,* pp. 140-149, 1999.

[5] 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.

[6] 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.

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

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

[9] C. J. Colbourn and J. H. Dinitz, *The Handbook of Combinatorial Designs*, Chapman & Hall/CRC, 2007.

[10] 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.

[11] 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.

[12] R. C. Bose and S. Chowla, "Theorems in the additive theory of numbers," *Commentarii Math-ematici Helvetici,* pp. 141-147, 1963.

[13] K. Drakakis, "A review of the available construction methods for Golomb rulers," *Adv. Math. Commun.,* vol. 3, no. 3, pp. 235-250, 2009.

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