

Regular Simplex Fingerprints and Their Optimality Properties

Negar Kiyavash¹ and Pierre Moulin^{2*}

¹ Coordinated Science Laboratory, Dept. of Electrical and Computer Engineering,
University of Illinois at Urbana-Champaign

kiyavash@uiuc.edu,

² Beckman Institute, Dept. of Electrical and Computer Engineering, University of
Illinois at Urbana-Champaign

moulin@ifp.uiuc.edu

Abstract. This paper addresses the design of additive fingerprints that are maximally resilient against Gaussian averaging collusion attacks. The detector performs a binary hypothesis test in order to decide whether a user of interest is among the colluders. The encoder (fingerprint designer) is to imbed additive fingerprints that maximize the probability of detecting at least one of the colluders. Both the encoder and the attackers are subject to squared-error distortion constraints. We show that n -Simplex Fingerprints are optimal in sense of maximizing a geometric figure of merit for the detection test; these fingerprints outperform orthogonal fingerprints. They are also optimal in terms of maximizing the error exponent of the detection test, and maximizing the deflection criteria at the detector when the attacker's noise is non-Gaussian. Reliable detection is guaranteed provided that the number of colluders $K \ll \sqrt{N}$, where N is the length of the host vector.

Key words. Fingerprinting, Simplex codes, Error exponents.

1 Introduction

Protection of digital property is an emerging need in light of growth of digital media and communication systems. Digital fingerprinting schemes are an important class of techniques devised for traitor tracing. In our view of digital fingerprinting, copyright protection is implicitly achieved through deterring users from illegally redistributing the digital content. Unlike watermarking where only one copy of the marked signal is circulated, in digital fingerprinting each user is provided with his own individually marked copy of the content. Although this makes it possible to trace an illegal copy to a traitor, it also allows for users to collude and form a stronger attack. One form of such attacks is averaging their copies and

* This work was supported by NSF grant CCR03-25924.

adding white Gaussian noise to create a *forgery*. The averaging reduces the power of each fingerprint and makes the detector's task harder.

Collusion-resistant fingerprints have been developed for various types of data, including binary sequences [1] and vectors in N -dimensional Euclidean spaces [2, 3]. According to Kilian *et al* [2], randomly generated Gaussian fingerprints can survive collusion of up to $O(\sqrt{N/\ln L})$ users, where L is the total number of fingerprints. The paper by Ergun *et al* [3] shows (under some assumptions) that any fingerprinting system can be defeated under collusion of $O(\sqrt{N/\ln N})$ users. In the aforementioned papers, the detector returns the index of one guilty user. Of course, the kind of decision to be made by the detector impacts the collusion resistance. A very hard problem for the detector, for instance, is to return a reliable list of all guilty users.

Other work on Gaussian fingerprints includes [4], which presents a game-theoretic analysis of the problem; the host signal, fingerprints and attack channel are all assumed to be Gaussian, and *all users* are assumed to collude. It is shown that the error exponent of the detector decreases as $1/L$. The performance of orthogonal Gaussian fingerprints is analyzed in [5], where upper and lower bound on the number of colluders that takes the detector to fail, are derived. One may ask whether either orthogonal or Gaussian fingerprints have any optimality property; this question has not yet been answered in the literature, so it is conceivable that some fingerprints constellations might be superior to orthogonal or random constellations.

In our problem setup, the detector has access to the host signal (non-blind detection) and performs a *binary hypothesis test* to verify whether a user of interest is colluding. The main contribution of this paper is a proof that regular simplex fingerprints are optimal in a certain minimum distance sense for the class of attacks considered. We also quantify the probability of error performance of our detector. In particular, they outperform orthogonal fingerprints; however the performance gap vanishes for large L .

The organization of the paper is as follows. In Section 2 we describe the attack channel and the notion of *focused* detector. In Section 3, we compute an upper bound on the performance of a given constellation of fingerprints. The main result of the paper is Theorem 2 of Section 4. In Section 5 we study the performance of a constellation against size- k coalition, where number of colluders K is less than the number of available prints L . We shall consider the joint fingerprinting and watermarking of

a host signal in Section 6. Finally we analyze the probability of error performance of our detector for size- k coalitions in Section 7.

2 Gaussian Fingerprints

In this section we describe the mathematical setup of the problem. The host signal is a sequence $\mathbf{S} = (S(1), \dots, S(N))$ in \mathbb{R}^N . Then L fingerprints, each of length N , are added to the host signal \mathbf{S} , where $L \leq N$ is the number of the users. In fact, typically we have $L \ll N$. User j is assigned a printed copy

$$\mathbf{X}_j = \mathbf{S} + \mathbf{Q}_j, \quad j \in \{1, \dots, L\}$$

where \mathbf{Q}_j denotes the fingerprint assigned to user j . Moreover there is a power constraint on the fingerprints, $\|\mathbf{Q}_j\|^2 \leq N$. The power constraint imposes a unit per-sample squared-error distortion,

$$\|\mathbf{X}_j - \mathbf{S}\|^2 \leq N. \quad (1)$$

To simplify the analysis, we restrict the attack channel to collusion between a subset of users in form of averaging their marked signals and subsequently contaminating the average with i.i.d Gaussian noise. The resulting illegal copy is of form

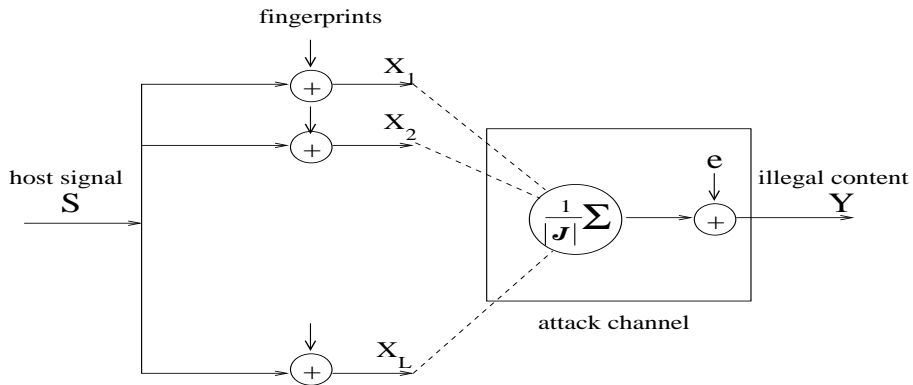


Fig. 1. Additive fingerprints and the averaging-plus-noise attack channel.

$$\mathbf{Y} = \mathbf{S} + \frac{1}{|\mathcal{J}|} \sum_{j \in \mathcal{J}} \mathbf{Q}_j + \mathbf{e}$$

where \mathcal{J} , the *coalition*, is the index set of the colluding users, and \mathbf{e} is an i.i.d. $\mathcal{N}(0, \sigma_e^2)$ Gaussian noise vector. We denote by $|\mathcal{J}|$ the cardinality of the set \mathcal{J} . Clearly $|\mathcal{J}| \leq L$. The host signal \mathbf{S} is available at the detector and can be subtracted from \mathbf{Y} . Thus

$$\mathbf{Y} - \mathbf{S} \sim \mathcal{N} \left(\frac{1}{|\mathcal{J}|} \sum_{j \in \mathcal{J}} \mathbf{Q}_j, \sigma_e^2 \right). \quad (2)$$

The detector performs a binary hypothesis test determining whether a certain user's mark is present in \mathbf{Y} . We shall denote the null or innocent hypothesis by H_0 while H_1 denotes the guilty hypothesis. We shall call this detector *focused*, because it decides whether a particular user of interest is a colluder. It does not aim at identifying all colluders. The *focused* detector above does not even need to know $|\mathcal{J}|$, the number of the colluders. Figure 1 depicts the fingerprinting process and the attack channel.

Since the total number of fingerprints is L , the detector can project the vector $(\mathbf{Y} - \mathbf{S}) \in \mathbb{R}^N$ onto the L -dimensional subspace spanned by $\{\mathbf{Q}_j\}_{j=1}^L$ ¹. The projection of $\mathbf{Y} - \mathbf{S}$ onto this subspace is a sufficient statistic for the detection. It is convenient to normalize this projection as follows:

$$\mathbf{V} \triangleq \frac{1}{\sqrt{N}} \text{Proj}[\mathbf{Y} - \mathbf{S}] \quad (3)$$

where $\text{Proj}[\cdot]$ denotes orthogonal projection onto the L -dimensional subspace of \mathbb{R}^N spanned by $\{\mathbf{Q}_j\}_{j=1}^L$. The vector \mathbf{V} is Gaussian with

$$\mathbf{V} \sim \mathcal{N} \left(\frac{1}{|\mathcal{J}|} \sum_{j \in \mathcal{J}} \mathbf{P}_j, \frac{1}{N} \sigma_e^2 \right) \quad (4)$$

where

$$\mathbf{P}_j \triangleq \frac{1}{\sqrt{N}} \text{Proj}[\mathbf{Q}_j] \in \mathbb{R}^L$$

and $\|\mathbf{P}_j\|^2 = 1$. We refer to $\pi = \{\mathbf{P}_j\}_{j=1}^L$ as the constellation of fingerprints on the L -dimensional unit sphere.

¹ If the dimension of span $\{\mathbf{Q}_j\}_{j=1}^L$ is less than L , then we can choose an arbitrary L dimensional embedding of subspace containing $\{\mathbf{Q}_j\}_{j=1}^L$.

In the rest of the paper we will work with fingerprints $\{\mathbf{P}_j\}_{j=1}^L$. To illustrate the binary hypothesis testing at the detector, we present an example of a decision problem with three printed copies.

Example 1. Assume three fingerprinted copies $\mathbf{X}_j = \mathbf{S} + \mathbf{Q}_j$, $j = 1, 2, 3$. In light of (3), the detector forms the sufficient statistic \mathbf{V} . Without loss of generality, assume the detector wants to decide whether user 1 is guilty. Any combination of fingerprints in which \mathbf{P}_1 is present implies that user 1 was one of the colluders. In light of (4), this corresponds to the case that the mean of \mathbf{V} is any of the entries of the left column in Table 1. On the other hand, if user 1 is not colluding, the mean of \mathbf{V} must be one of the entries of the right column.

User 1 Guilty	User 1 Not Guilty
\mathbf{P}_1	\mathbf{P}_2
$\frac{1}{2}(\mathbf{P}_1 + \mathbf{P}_2)$	\mathbf{P}_3
$\frac{1}{2}(\mathbf{P}_1 + \mathbf{P}_3)$	$\frac{1}{2}(\mathbf{P}_2 + \mathbf{P}_3)$
$\frac{1}{3}(\mathbf{P}_1 + \mathbf{P}_2 + \mathbf{P}_3)$	

Table 1. Detector's binary decision sets \mathcal{G}_1 and $-\mathcal{G}_1$ for three colluders: $\mathcal{J} = \{1, 2, 3\}$.

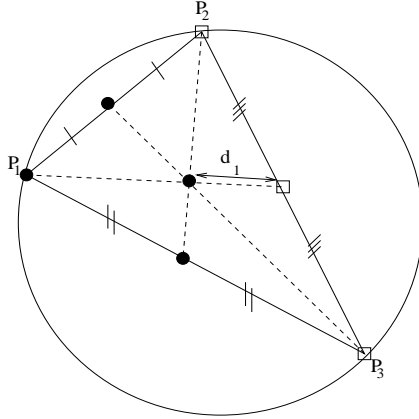


Fig. 2. A constellation of fingerprints for three users. The four bullets correspond to the elements of \mathcal{G}_1 , while the three elements of set $-\mathcal{G}_1$ are represented by squares.

The entries of the table are vectors in \mathbb{R}^L . The vectors in the left column form a set \mathcal{G}_1 corresponding to the guilty hypothesis. The vectors that correspond to a not-guilty assumption form the set $\neg\mathcal{G}_1$. For a fixed user j , let

$$d_j \triangleq \text{dist}(\mathcal{G}_j, \neg\mathcal{G}_j) = \min_{(g, g') \in \mathcal{G}_j \times \neg\mathcal{G}_j} \|g - g'\| \quad (5)$$

be the smallest distance between the sets \mathcal{G}_j and $\neg\mathcal{G}_j$, e.g. d_1 is the smallest distance among the 12 possible distances between the entries of Table 1. Figure 2 depicts a constellation of three prints.

The exact calculation of probability of error for signal constellations for all signal to noise ratios is not easy when the vectors \mathbf{P}_j are not orthogonal [6]. In channel coding problems, it is common to judge a constellation by its minimum distance [7], [8]. Here the appropriate figure of merit for a detector focused on user j is d_j .

However a good constellation must perform well regardless of which user is the person of the interest to detector. Hence we would like to choose a constellation that has the overall largest minimum distance. More precisely, we call

$$d_\pi = \min_{1 \leq j \leq L} d_j \quad (6)$$

the *minimum distance of the constellation* π . We wish to choose π that maximizes d_π . For Example 1, $d_\pi = \min(d_1, d_2, d_3)$. Note here that we assume all users are potential colluders, i.e., we may have $\mathcal{J} = \{1, \dots, L\}$.

Definition 1. *Let π^* be a maximizer of d_π . The fingerprints obtained from π^* are called *Optimal Focused Fingerprints (OFF)*.*

Next we will show that OFF constellations can be found for any number $L \leq N$ of users.

3 Optimal Focused Fingerprints

In this section we derive an achievable upper bound for d_π . Let

$$\mathcal{S}^{L-1} = \{\mathbf{P} \in \mathbb{R}^L : \|\mathbf{P}\| = 1\}$$

denote the unit sphere in \mathbb{R}^{L-1} . Moreover the centroid of a constellation $\{\mathbf{P}_j\}_{j=1}^L$ is defined as $\frac{1}{L} \sum_{j=1}^L \mathbf{P}_j$. We derive necessary and sufficient conditions for L points on the sphere to maximize the sum of their mutual squared distances.

Lemma 1. Any constellation of L points on \mathcal{S}^{L-1} with its centroid at origin, maximizes the sum $\sum_{1 \leq i < j \leq L} \|\mathbf{P}_i - \mathbf{P}_j\|^2$. The maximum is equal to L^2 .

Proof. We have

$$\begin{aligned} \sum_{1 \leq i < j \leq L} \|\mathbf{P}_i - \mathbf{P}_j\|^2 &= \sum_{1 \leq i < j \leq L} \|\mathbf{P}_i\|^2 + \|\mathbf{P}_j\|^2 - 2\langle \mathbf{P}_i, \mathbf{P}_j \rangle \\ &= \sum_{1 \leq i < j \leq L} 2 - 2\langle \mathbf{P}_i, \mathbf{P}_j \rangle \\ &= L(L-1) - 2 \sum_{1 \leq i < j \leq L} \langle \mathbf{P}_i, \mathbf{P}_j \rangle. \end{aligned} \quad (7)$$

Also

$$\begin{aligned} \left\| \sum_{i=1}^L \mathbf{P}_i \right\|^2 &= \sum_{i=1}^L \|\mathbf{P}_i\|^2 + 2 \sum_{i < j} \langle \mathbf{P}_i, \mathbf{P}_j \rangle \\ &= L + 2 \sum_{i < j} \langle \mathbf{P}_i, \mathbf{P}_j \rangle. \end{aligned} \quad (8)$$

Combining (7) and (8), we obtain the upper bound

$$\sum_{1 \leq i < j \leq L} \|\mathbf{P}_i - \mathbf{P}_j\|^2 = L^2 - \left\| \sum_{i=1}^L \mathbf{P}_i \right\|^2 \leq L^2.$$

The upper bound is achieved when the centroid is at the origin. \square

Theorem 1. For any constellation π of L fingerprints on \mathcal{S}^{L-1} , we have

$$d_\pi \leq \frac{1}{L-1}.$$

Moreover any constellation π with its centroid at the origin achieves the upper bound, and therefore is OFF.

Proof. Again let d_j denote the smallest distance between the points of \mathcal{G}_j and $\neg\mathcal{G}_j$. Since by definition $d_\pi \leq \min_j d_j$, we obtain

$$d_\pi^2 \leq \frac{1}{L} \sum_{j=1}^L d_j^2. \quad (9)$$

Furthermore it can be shown that (details are lengthy and therefore are omitted) d_j , the smallest distance between the sets \mathcal{G}_j and $\neg\mathcal{G}_j$, is achieved by the pair $\left(\frac{1}{L}\sum_{i=1}^L \mathbf{P}_i, \frac{1}{L-1}\sum_{i \neq j} \mathbf{P}_i\right)$, thus we have

$$d_j = \left\| \frac{1}{L(L-1)} \left[(L-1)\mathbf{P}_j - \sum_{i \neq j} \mathbf{P}_i \right] \right\| = \frac{1}{L(L-1)} \left\| \sum_{i \neq j} (\mathbf{P}_i - \mathbf{P}_j) \right\|. \quad (10)$$

Substituting d_j from (10) into (9) we have,

$$\begin{aligned} d_\pi^2 &\leq \frac{1}{L} \sum_{j=1}^L \frac{1}{L^2(L-1)^2} \left\| \sum_{i \neq j} (\mathbf{P}_i - \mathbf{P}_j) \right\|^2 \\ &= \frac{1}{L^3(L-1)^2} \left[\sum_{i \neq 1} \|\mathbf{P}_i - \mathbf{P}_1\|^2 + 2 \sum_{i < j} \langle \mathbf{P}_i - \mathbf{P}_1, \mathbf{P}_j - \mathbf{P}_1 \rangle + \dots \right. \\ &\quad \left. + \sum_{i \neq L} \|\mathbf{P}_i - \mathbf{P}_L\|^2 + 2 \sum_{i < j} \langle \mathbf{P}_i - \mathbf{P}_L, \mathbf{P}_j - \mathbf{P}_L \rangle \right]. \end{aligned}$$

Regrouping terms we have,

$$d_\pi^2 \leq \frac{1}{L^3(L-1)^2} \left[2 \sum_{i < j} \|\mathbf{P}_i - \mathbf{P}_j\|^2 + 2 \sum_{k=1}^L \sum_{i < j} \langle \mathbf{P}_i - \mathbf{P}_k, \mathbf{P}_j - \mathbf{P}_k \rangle \right]. \quad (11)$$

For any fixed triple (k, i, j) , there is a term of the form $\langle \mathbf{P}_i - \mathbf{P}_k, \mathbf{P}_j - \mathbf{P}_k \rangle$ in the sum, now depending on whether $k < j$ or $k > j$ either $\langle \mathbf{P}_k - \mathbf{P}_i, \mathbf{P}_j - \mathbf{P}_i \rangle$ or its equivalent $\langle \mathbf{P}_j - \mathbf{P}_i, \mathbf{P}_k - \mathbf{P}_i \rangle$ belongs to the sum as well. But $\langle \mathbf{P}_i - \mathbf{P}_k, \mathbf{P}_j - \mathbf{P}_k \rangle + \langle \mathbf{P}_k - \mathbf{P}_i, \mathbf{P}_j - \mathbf{P}_i \rangle = \langle \mathbf{P}_i - \mathbf{P}_k, \mathbf{P}_j - \mathbf{P}_k + (\mathbf{P}_i - \mathbf{P}_j) \rangle$ which in turn equals $\|\mathbf{P}_i - \mathbf{P}_k\|^2$.

For each user k , \mathbf{P}_k is fixed and there are $\frac{1}{2}(L-1)(L-2)$ terms in $\sum_{i < j} \langle \mathbf{P}_i - \mathbf{P}_k, \mathbf{P}_i - \mathbf{P}_k \rangle$. But then summing this again over k results in $\frac{1}{2}L(L-1)(L-2)$ terms of the form $\|\mathbf{P}_i - \mathbf{P}_k\|^2$. Now grouping this with the other terms of the form $\sum_{i < j} \|\mathbf{P}_i - \mathbf{P}_j\|^2$, will have a contribution of $\frac{\frac{1}{2}L(L-1)(L-2)}{\frac{1}{2}L(L-1)} = L-2$ new terms. Substituting this into (11) we have

$$\begin{aligned}
d_\pi^2 &\leq \frac{1}{L^3(L-1)^2} \left[2 \sum_{i<j} \|\mathbf{P}_i - \mathbf{P}_j\|^2 + (L-2) \sum_{i<j} \|\mathbf{P}_i - \mathbf{P}_j\|^2 \right] \\
&= \frac{1}{L^2(L-1)^2} \sum_{i<j} \|\mathbf{P}_i - \mathbf{P}_j\|^2.
\end{aligned}$$

or

$$d_\pi \leq \frac{1}{L(L-1)} \sqrt{\sum_{i<j} \|\mathbf{P}_i - \mathbf{P}_j\|^2}. \quad (12)$$

From Lemma 1, $\sum_{i<j} \|\mathbf{P}_i - \mathbf{P}_j\|^2$ is maximized when the fingerprints form a constellation with its centroid at the origin. Combining this result with (12), we obtain $d_\pi \leq \frac{1}{L-1}$. \square

Theorem 1 states that the bound is achievable by any constellation with centroid at the origin.

4 n -Simplex Fingerprints

In this section we formally define n -Simplex Fingerprints. These fingerprints have their centroid at the origin and therefore are OFF.

Definition 2. [9] *A simplex, sometimes called a hypertetrahedron, is the generalization of a tetrahedral region of space to n dimensions. If all the 1-faces (polytope edges) in the simplex are equal, it is regular.*

In one dimension, the regular simplex is the line segment $[-1, +1]$. In two dimensions, the regular simplex is the equilateral triangle. In three dimensions, the regular simplex is the regular tetrahedron. The regular simplex in four dimensions (the pentatope) $ABCDE$ is obtained from the regular tetrahedron $ABCD$ by choosing a point E along the fourth dimension through the center of $ABCD$ so that $EA = EB = EC = ED = AB$. Similarly one can recursively construct a regular n -simplex from a regular $n-1$ -simplex, by choosing a new vertex along the n th dimension through the centroid of the existing $n-1$ -simplex, such that the new vertex is at equal distance from all the vertices of the $n-1$ -simplex.

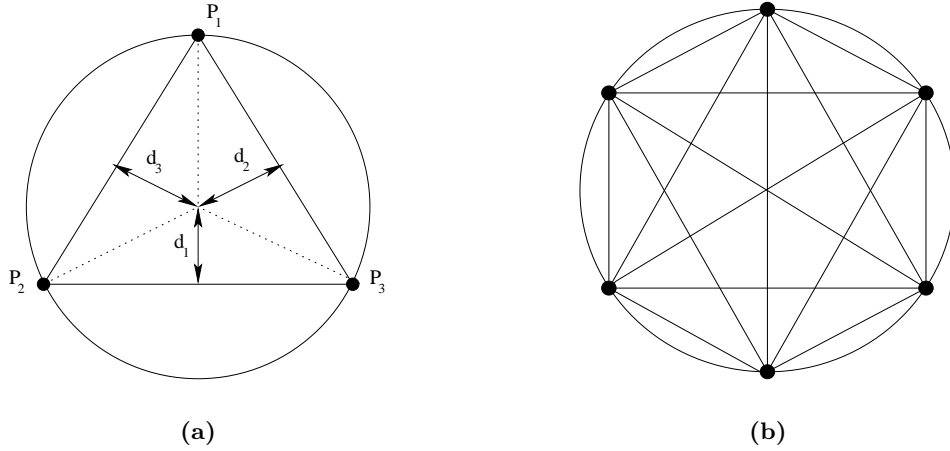


Fig. 3. (a) Planar graph representation for 2-simplex. (b) Planar graph representation for 5-simplex.

It is convenient to describe a simplex in barycentric coordinates. The vertices of the simplex in barycentric coordinates can be expressed as $(1, 0, 0, \dots, 0)$, $(0, 1, 0, \dots, 0)$, \dots , $(0, 0, 0, \dots, 1)$. There exists a planar graph representation for n -simplices. Figure 3 depicts the complete graph corresponding to 2 and 5-simplices.

Regular n -polytopes and thus the regular n -simplex may be inscribed in centered n -spheres; the smallest such sphere is called the circumsphere. In fact, there is an n -sphere touching the centers of all the elements bounding the n -polytope: vertices, edges, faces and polyhedra.

This property is essential for us. By the power constraint $\|\mathbf{P}_j\|^2 = 1$, our fingerprints are to lie on an L -dimensional sphere. In light of Theorem 1 the following theorem is immediate.

Theorem 2. *Under the Gaussian averaging attack of section 2, the L vertices of the $(L - 1)$ -simplex inscribed inside the unit sphere \mathcal{S}^{L-1} form an OFF constellation for L users. Moreover, all the distances d_j , $1 \leq j \leq L$, are equal to $\frac{1}{L-1}$. The property $d_j \equiv d_\pi$ follows from the symmetry of the regular simplex.*

Proof. Because the centroid of the regular simplex is at the origin, the $(L - 1)$ -simplex achieves the upper bound of Theorem 1 on d_π and thus its L vertices form an OFF constellation. \square

5 Size-K Coalitions

Although minimum distance d_π of Equation (6) is our basic figure of merit for constellation design, it is often necessary to study the performance of a scheme when at most K out of L potential colluders form the attack. $|\mathcal{J}| \leq K$. Table 2 shows the modification of the sets \mathcal{G}_j and $\neg\mathcal{G}_j$ of Example 1 for a coalition of size at most $K = 2$.

User 1 Guilty	User 1 Not Guilty
\mathbf{P}_1	\mathbf{P}_2
$\frac{1}{2}(\mathbf{P}_1 + \mathbf{P}_2)$	\mathbf{P}_3
$\frac{1}{2}(\mathbf{P}_1 + \mathbf{P}_3)$	$\frac{1}{2}(\mathbf{P}_2 + \mathbf{P}_3)$

Table 2. Detector's binary decision sets \mathcal{G}_1 and $\neg\mathcal{G}_1$ when there are at most $K = 2$ colluders.

Let's assume the the user of interest is \mathbf{P}_j and the attackers have formed a size- K coalition, i.e. $|\mathcal{J}| = K$. Similarly to Equation 5, the minimum distance between the two sets \mathcal{G}_j and $\neg\mathcal{G}_j$ is

$$\text{dist}(\mathcal{G}_j, \neg\mathcal{G}_j) = \min_{(g, g') \in \mathcal{G}_j \times \neg\mathcal{G}_j} \|g - g'\|. \quad (13)$$

Assuming $K < L$, this distance is achieved by the pair of forgeries $(\mathbf{F}_1, \mathbf{F}'_1)$, where

$$\mathbf{F}_1 = \frac{1}{K} \sum_{i \in \mathcal{J}} \mathbf{P}_i, \quad \mathbf{F}'_1 = \frac{1}{K} \left(\sum_{i \in \mathcal{J} \setminus \{j\}} \mathbf{P}_i + \mathbf{P}_k \right), \quad (14)$$

where k is any index that is not present in the coalition \mathcal{J} .

6 Fingerprinting Watermarked Data

Digital fingerprinting schemes are devised for traitor tracing. However it might be necessary to insert a watermark to protect the rights to the ownership of the original content. One way of achieving this joint watermarking and fingerprinting scheme is to first add watermark \mathbf{W} to the content and then add the fingerprints,

$$\mathbf{X}_j = \mathbf{S} + \mathbf{W} + \mathbf{Q}_j, \quad j \in \{1, \dots, L\}.$$

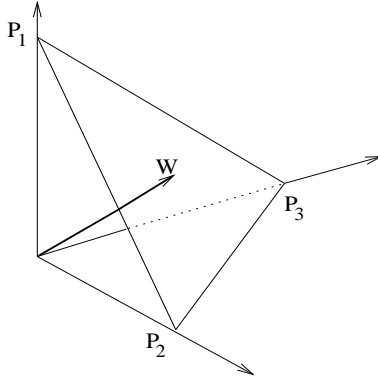


Fig. 4. Additive joint fingerprint and watermark constellation.

A natural choice for the watermark signal is to be perpendicular to the the span of the fingerprints: $\mathbf{W} \perp \text{Span}\{Q_j\}$. This choice implies that averaging the copies \mathbf{X}_j cannot degrade the watermark \mathbf{W} .

For the *focused* detector of Section 2, Figure 4 depicts the signal constellation for joint fingerprints and the watermark. Observe that the distortion constraint of Equation (1) implies that there is less power available for the fingerprints \mathbf{Q}_j :

$$\|\mathbf{W}\|^2 + \|\mathbf{Q}_j\|^2 \leq N \quad j \in \{1, \dots, L\}.$$

Thus, there is a tradeoff between the power allocated to the watermark \mathbf{W} and the power of the prints \mathbf{Q}_j . The fingerprints still are chosen to be the vertices of an $L-1$ -simplex, where L is the number of the fingerprints, but they are circumscribed in a smaller sphere. As an special case, in the L -dimensional space one can allocate the power between \mathbf{W} and the fingerprints \mathbf{Q}_j such that the resulting fingerprints are orthogonal. Note that $\|\mathbf{W}\|^2 \rightarrow 0$ as $L \rightarrow \infty$ in this case.

7 Probability of Error

The performance metric d_π in this paper is a geometric figure of merit for fingerprint constellations. From a detection standpoint however, the most natural performance criterion is $P_e(\pi)$, the *maximal probability of error of the focused detector* over all size K coalitions. Assume that the detector is focused on user j . Our detector forms the following correlation statistic:

$$T(\mathbf{Y}) = \mathbf{P}_j^T(\mathbf{Y} - \mathbf{S}) \underset{H_0}{\overset{H_1}{\gtrless}} \tau. \quad (15)$$

The decision boundary for this test is a hyperplane normal to the vector \mathbf{P}_j :

$$\Omega = \{\mathbf{Y} : \mathbf{P}_j^T(\mathbf{Y} - \mathbf{S}) = \tau\}.$$

Assume without loss of generality that the detector is focused on user 1 ($j = 1$), and that $\mathcal{J} = \{1, 2, \dots, K\}$. For the forgery \mathbf{F}_1 defined in (14), we have

$$\begin{aligned} T(\mathbf{Y}) &= \mathbf{P}_1^T \mathbf{F}_1 \\ &= \frac{1}{K} \sum_{i=1}^K \mathbf{P}_1^T \mathbf{P}_i \\ &= \frac{1}{K} \left(1 - \frac{K-1}{L-1} \right) \\ &= \frac{L-K}{K(L-1)} \triangleq \tau_{\max}. \end{aligned} \quad (16)$$

Similarly, for the forgery \mathbf{F}'_1 , we have

$$\begin{aligned} T(\mathbf{Y}) &= \mathbf{P}_1^T \mathbf{F}'_1 \\ &= \frac{1}{K} \sum_{i=2}^{K+1} \mathbf{P}_1^T \mathbf{P}_i \\ &= -\frac{1}{L-1} \triangleq \tau_{\min}. \end{aligned} \quad (17)$$

If $\tau \geq \tau_{\max}$, the focused detector incorrectly decides H_0 upon seeing forgery \mathbf{F}_1 . The worst-case probability of miss P_M is equal to 1. Likewise, if $\tau \leq \tau_{\min}$, the focused detector incorrectly decides H_1 upon seeing forgery \mathbf{F}'_1 . The worst-case probability of false alarm P_F is equal to 1.

The threshold τ trades off P_F and P_M . To minimize probability of error, τ should be chosen as

$$\tau = \frac{\tau_{\min} + \tau_{\max}}{2} = \frac{L - 2K}{2K(L - 1)}.$$

The relevant figure of merit for this test is

$$d_\pi(K) \triangleq \tau_{\max} - \tau_{\min} = \frac{L}{K(L-1)}. \quad (18)$$

Note that $d_\pi(K) \downarrow \frac{1}{K}$ as $L \rightarrow \infty$, and $\tau \uparrow \frac{1}{2K}$ as $\frac{L}{K} \rightarrow \infty$.

The significance of $d_\pi(K)$ in this context is as follows:

- For any constellation π , we have

$$P_e(\pi) = Q\left(\frac{\sqrt{N}d_\pi(K)}{2\sigma}\right),$$

where $Q(t) \triangleq \int_t^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} dx$ is the Q function. Recall that for positive t , the Q function is bounded by $\frac{1}{t\sqrt{2\pi}} e^{-\frac{t^2}{2}} \leq Q(t) \leq e^{-\frac{t^2}{2}}$. Moreover $\ln Q(t) \sim e^{-\frac{t^2}{2}}$ as $t \rightarrow \infty$.

- The error exponent of the detection test, for any fixed K , is

$$e(\pi) \triangleq -\lim_{N \rightarrow \infty} \frac{1}{N} \ln P_e(\pi) = -\lim_{N \rightarrow \infty} \frac{1}{N} \ln Q\left(\frac{\sqrt{N}d_\pi(K)}{2\sigma}\right) = \frac{d_\pi^2(K)}{8\sigma^2}.$$

- If the noise \mathbf{e} is non-Gaussian, $d_\pi(K)$ represents the *deflection criterion*, or generalized SNR [10], of the test.

It is noteworthy that as the number of colluders $K \rightarrow \infty$, the quantity

$$\frac{d_\pi^2(K)}{8\sigma^2} = \frac{\left(\frac{L}{L-1}\right)^2}{8\sigma^2 K^2} \sim \frac{1}{4\sigma^2 K^2}$$

tends to zero. Hence the error exponent $e(\pi)$ is zero. Still, provided $K \ll \sqrt{N}$, the probability of error goes to zero:

$$P_e(\pi) = Q\left(\frac{\sqrt{N}d_\pi(K)}{2\sigma}\right) = Q\left(\frac{\sqrt{N}\frac{L}{L-1}}{2\sigma K}\right)$$

thus,

$$\begin{aligned} & \left(\sqrt{2\pi}\frac{\sqrt{N}\frac{L}{L-1}}{2\sigma K}\right)^{-1} \exp\left(-\frac{NL^2}{8\sigma^2 K^2(L-1)^2}\right) \\ & \leq Q\left(\frac{\sqrt{N}\frac{L}{L-1}}{2\sigma K}\right) \leq \exp\left(-\frac{NL^2}{8\sigma^2 K^2(L-1)^2}\right) \end{aligned}$$

which implies $P_e(\pi) \rightarrow 0$.

However, when K is of the order of \sqrt{N} , $P_e(\pi)$ does not vanish as $N \rightarrow \infty$; and if $K \gg N$, $P_e(\pi)$ tends to $\frac{1}{2}$.

For large N , our optimal $d_\pi = \frac{1}{L-1}$ converges to $d_\pi = \frac{1}{L}$ that was derived in [4] under different assumptions: random design of the fingerprints (statistically orthogonal), and all users colluding. Moreover as shown in [5] geometrically orthogonal fingerprint designs achieve the same $d_\pi = \frac{1}{L}$.

8 Acknowledgements

The authors wish to thank Professor Peter Dragnev and Professor Richard E. Blahut for helpful comments.

References

1. D. Boneh and J. Shaw. Collusion-secure fingerprinting for digital data. In Don Coppersmith, editor, *Proc. Crypto '95*, pages 452–465. Springer, 1995. Lecture Notes in Computer Science No. 963.
2. J. Kilian, F.T. Leighton, L.R. Matheson, T.G. Shamoan, R.E. Tarjan, and F. Zane. Resistance of digital watermarks to collusive attacks. In *IEEE International Symposium on Information Theory*, page 271, 1998.
3. F. Ergun, J. Kilian, and R. Kumar. A note on the bounds of collusion resistant watermarks. In *EUROCRYPT'99*, pages 140–149, 1999.
4. P. Moulin and A. Briassouli. The Gaussian fingerprinting game. *Conference on Information Sciences and Systems, CISS'02*, March 2002.
5. Z. Wang, M. Wu, H. Zhao, W. Trappe, , and K.J.R. Liu. Collusion resistance of multimedia fingerprinting using orthogonal modulation. *IEEE Trans. on Image Proc.*, To appear June 2005.
6. H.V. Poor. *An Introduction to Signal Detection and Estimation*. Springer-Verlang, 2nd edition, 1994.
7. R. Blahut. *An Introduction to Telecommunications*. Cambridge University Press, Cambridge. Preprint.
8. Jr. Forney, G.D. and L.-F. Wei. Multidimensional constellations. I. introduction, figures of merit, and generalized cross constellations. *IEEE Journal on Selected Areas in Communications*, 7(6):877 – 892, 1989.
9. J. R. Munkres. *Elements of Algebraic Topology*. Perseus Press, 1993.
10. R. J. Barton and H. V. Poor. On generalized signal-to-noise ratios in signal detection. *Mathematics of Control, Signals and Systems*, 5(1):81 – 91, 1992.