EURASIP Journal on Applied Signal Processing 2004:14, 2142–2162

Group-Oriented Fingerprinting for Multimedia Forensics

Z. Jane Wang
Department of Electrical and Computer Engineering, University of British Columbia, 2356 Main Mall, Vancouver, BC, Canada V6T 1Z4
Email: zjanew@ece.ubc.ca

Min Wu
Department of Electrical and Computer Engineering and Institute for Systems Research, University of Maryland, College Park, MD 20742, USA
Email: minwu@eng.umd.edu

Wade Trappe
Wireless Information Network Laboratory (WINLAB) and the Electrical and Computer Engineering Department, Rutgers University, NJ 08854–8060, USA
Email: trappe@winlab.rutgers.edu

K. J. Ray Liu
Department of Electrical and Computer Engineering and Institute for Systems Research, University of Maryland, College Park, MD 20742, USA
Email: kjrliu@eng.umd.edu

Received 7 April 2003; Revised 15 September 2003

Digital fingerprinting of multimedia data involves embedding information in the content signal and offers protection to the digital rights of the content by allowing illegitimate usage of the content to be identified by authorized parties. One potential threat to fingerprinting is collusion, whereby a group of adversaries combine their individual copies in an attempt to remove the underlying fingerprints. Former studies indicate that collusion attacks based on a few dozen independent copies can confound a fingerprinting system that employs orthogonal modulation. However, in practice an adversary is more likely to collude with some users than with other users due to geographic or social circumstances. To take advantage of prior knowledge of the collusion pattern, we propose a two tier group-oriented fingerprinting scheme where users likely to collude with each other are assigned correlated fingerprints. Additionally, we extend our construction to represent the natural social and geographic hierarchical relationships between users by developing a more flexible tree structure-based fingerprinting system. We also propose a multistage colluder identification scheme by taking advantage of the hierarchial nature of the fingerprints. We evaluate the performance of the proposed fingerprinting scheme by studying the collusion resistance of a fingerprinting system employing Gaussian-distributed fingerprints. Our results show that the group-oriented fingerprinting system provides the superior collusion resistance over a system employing orthogonal modulation when knowledge of the potential collusion pattern is available.

Keywords and phrases: multimedia fingerprinting, multimedia forensics, collusion resistance, group-oriented fingerprinting, multistage colluder identification.

1. INTRODUCTION AND PROBLEM DESCRIPTION

With the rapid deployment of multimedia technologies and the substantial growth in the use of the Internet, the protection of digital multimedia data has become increasingly critical to the welfare of many industries. Protecting multimedia content cannot rely merely upon classical security mechanisms, such as encryption, since the content must ultimately be decrypted prior to rendering. These cleartext representations are available for adversaries to repackage and redistribute, and therefore additional protection mechanisms are needed to discourage unauthorized redistribution. One mechanism that complements encryption is the fingerprinting of multimedia, whereby tags are embedded in multimedia content. Whereas data encryption seeks to prevent unauthorized access to data, digital fingerprinting is a

forensic technology that provides a mechanism for identifying the parties involved in unauthorized usage of content. By providing evidence to content owners or digital rights enforcement agencies that substantiates the guilt of parties involved in the improper use of content, fingerprinting ultimately discourages fraudulent behavior.

However, in order for multimedia fingerprinting to provide a reliable measure of security, it is necessary that the fingerprints can withstand attacks aimed at removing or destroying the embedded information. Many embedding techniques have been proposed that are capable of withstanding traditional attacks mounted by individuals, such as filtering and compression. However, with the proliferation of communication networks, the effective distance between adversaries has decreased and it is now feasible for attacks to be mounted by groups instead of merely by individuals. Such attacks, known as *collusion* attacks, are a class of cost-effective and powerful attacks whereby a coalition of users combine their different marked copies of the same media content for the purpose of removing the original fingerprints. Fingerprinting must therefore survive both standard distortion attacks as well as collusion attacks.

Several methods have been proposed in the literature to embed and hide fingerprints in different media through watermarking techniques [1, 2, 3, 4, 5, 6]. The spread spectrum watermarking method, where the watermarks have a componentwise Gaussian distribution and are statistically independent, has been argued to be highly resistant to classical attacks [2].

The research on collusion-resistant fingerprinting systems involve two main directions of study: designing collusion-resistant fingerprint codes [7, 8, 9, 10, 11] and examining the resistance performance of specific watermarking schemes under different attacks [12, 13, 14, 15]. With a simple linear collusion attack that consists of adding noise to the average of K independent copies, it was concluded in [13] that, for n users and fingerprints using N samples, $O(\sqrt{N/\log n})$ independently marked copies are sufficient for an attack to defeat the underlying system with nonnegligible probability, when Gaussian watermarks are considered. Gaussian watermarks were further shown to be optimal: no other watermarking scheme can offer better collusion resistance [13]. These results are also supported by [12]. Stone reported a powerful collusion attack capable of defeating uniformly distributed watermarks that employs as few as one to two dozen independent copies of marked content [15]. In our previous work, we analyzed the collusion resistance of an orthogonal fingerprinting system under different collusion attacks for different performance criteria, and derived lower and upper bounds for the maximum number of colluders needed to thwart the system [16].

Despite the superior collusion resistance of orthogonal Gaussian fingerprints over other fingerprinting schemes, previous analysis revealed that attacks based on a few dozen independent copies can confound a fingerprinting system using orthogonal modulation [12, 13, 16]. Ultimately, for mass market consumption of multimedia, content will be distributed to thousands of users. In these scenarios, it is possible for a coalition of adversaries to acquire a few dozen copies of marked content, employ a collusion attack, and thereby thwart the protection provided by the fingerprints. Thus, an alternative fingerprinting scheme is needed that will exploit a different aspect of the collusion problem in order to achieve improved collusion resistance.

In this paper, we introduce a new direction for improving collusion resistance. We observe that some users are more likely to collude with each other than with other users, perhaps due to underlying social or cultural factors. We propose to exploit this a priori knowledge to improve the fingerprint design. We introduce a fingerprint construction that is an alternative to the traditional independent Gaussian fingerprints. Like the traditional spread-spectrum watermarking scheme, our fingerprints are Gaussian distributed. However, we assign statistically independent fingerprints to members of different groups that are unlikely to collude with each other, while the fingerprints we assign to members within a group of potential colluders are correlated.

We begin, in Section 2, by introducing our model for multimedia fingerprinting. Throughout this paper, we consider additive embedding, a general watermarking scheme whereby a watermark signal is added to a host signal. We then introduce the problem of user collusion, and focus our studies on the averaging form of linear collusion attacks. Further, in Section 2, we highlight the motivation for our group-oriented fingerprinting scheme. In Section 3, we present our construction of a two-tier fingerprinting scheme in which the groups of potential colluders are organized into sets of users that are equally likely to collude with each other. We assume, in the two-tier model that intergroup collusion is less likely than intragroup collusion. The design of the fingerprint is complemented by the development and analysis of a detection scheme capable of providing the forensic ability to identify groups involved in collusion and to trace colluders within each group. We extend our construction to more general group collusion scenarios in Section 4 by presenting a tree-based construction of fingerprints. In Section 3.3, we evaluate the performance of our fingerprinting schemes by providing experimental results using images. Finally, we present conclusions in Section 6, and provide proofs of various claims in the appendices.

2. FINGERPRINTING AND COLLUSION

In this section, we will introduce fingerprinting and collusion. Collusion-resistant fingerprinting requires the design of fingerprints that can survive collusion and identify colluders, as well as the robust embedding of the fingerprints in the multimedia host signal. We will employ spread spectrum additive embedding of fingerprints in this paper since this technique has proven to be robust against a number of attacks [2]. Additionally, information theory has shown that spread spectrum additive embedding is near optimal when the original host signal is available at the detector side [17, 18], which is a reasonable assumption for collusion applications.

We begin by reviewing spread spectrum additive embedding. Suppose that the host signal is represented by a vector $\mathbf{x}$, which might, for example, consist of the most significant discrete cosine transform (DCT) components of an image. The owner generates the watermark $\mathbf{s}$ and embeds each component of the watermark into the host signal by $y(l) = x(l)+s(l)$ with $y(l)$, $x(l)$, and $s(l)$ being the lth component of the watermarked copy, the host signal, and the watermark, respectively. It is worth mentioning that, in practical watermarking, before the watermark is added to the host signal, each component of the watermark $\mathbf{s}$ is scaled by an appropriate factor to achieve the imperceptibility of the embedded watermark as well as control the energy of the embedded watermark. One possibility for this factor is to use the *just-noticeable-difference* (JND) from a human visual model [19].

In digital fingerprinting, the content owner has a family of watermarks, denoted by $\{\mathbf{s}_j\}$, which are fingerprints associated with different users who purchase the rights to access the host signal $\mathbf{x}$. These fingerprints are used to make copies of content that may be distributed to different users, and allow for the tracing of pirated copies to the original users. For the jth user, the owner computes the marked version of the content $\mathbf{y}_j$ by adding the watermark $\mathbf{s}_j$ to the host signal, meaning $\mathbf{y}_j = \mathbf{x} + \mathbf{s}_j$. Then this fingerprinted copy $\mathbf{y}_j$ is distributed to user j and may experience additional distortion before it is tested for the existence of the fingerprint $\mathbf{s}_j$. The fingerprints $\{\mathbf{s}_j\}$ are often chosen to be orthogonal noise-like signals [2], or are built by using a modulation scheme employing a basis of orthogonal noise-like signals [11, 20]. For this paper, we restrict our attention to linear modulation schemes, where the fingerprint signals $\mathbf{s}_j$ are constructed using a linear combination of a total of v orthogonal basis signals $\{\mathbf{u}_i\}$ such that

$$\mathbf{s}_j = \sum_{i=1}^{v} b_{ij}\mathbf{u}_i, \tag{1}$$

and a sequence $\{b_{1j}, b_{2j}, \ldots, b_{vj}\}$ is assigned for each user j. It is convenient to represent $\{b_{ij}\}$ as a matrix $\mathcal{B}$, and different matrix structures correspond to different fingerprinting strategies. An identity matrix for $\mathcal{B}$ corresponds to orthogonal modulation [2, 21, 22], where $\mathbf{s}_j = \mathbf{u}_j$. Thus each user is identified by means of an orthogonal basis signal. In practice it is often sufficient to use independently generated random vectors $\{\mathbf{u}_j\}$ for spread spectrum watermarking [2]. The orthogonality or independence allows for distinguishing different users' fingerprints to the maximum extent. The simple structure of orthogonal modulation for encoding and embedding makes it attractive in identification applications that involve a small group of users. Fingerprints may also be designed using code modulation [23]. In this case, the matrix $\mathcal{B}$ takes a more general form. One advantage of using code modulation is that we are able to represent more than v users when using v orthogonal basis signals. One method for constructing the matrix $\mathcal{B}$ is to use appropriately designed binary codes. As an example, we recently proposed a class of binary-valued anticollusion codes (ACC), where the shared bits within code vectors allow for the identification of up to K colluders [11]. In more general constructions, the entries of $\mathcal{B}$ can be real numbers. The key issue of fingerprint design using code modulation is to strategically introduce correlation among different fingerprints to allow for accurate identification of the contributing fingerprints involved in collusion.

In a collusion attack on a fingerprinting system, one or more users with different marked copies of the same host signal come together and combine several copies to generate a new composite copy $\mathbf{y}$ such that the traces of each of the "original" fingerprints are removed or attenuated. Several types of collusion attacks against multimedia embedding have been proposed, such as nonlinear collusion attacks involving order statistics [15]. However, in a recent investigation we showed that different nonlinear collusion attacks had almost identical performance to linear collusion attacks based on averaging marked content signals, when the levels of mean square error (MSE) distortion introduced by the attacks were kept fixed. In a K-colluder averaging-collusion attack, the watermarked content signals $\mathbf{y}_j$ are combined according to $\sum_{j=1}^{K} \lambda_j \mathbf{y}_j + \mathbf{d}$, where $\mathbf{d}$ is an added distortion. Since no colluder would be willing to take higher risk than others, the λ_j are often chosen to be equal [10, 12, 13, 14]. For the simplicity of analysis, we will focus on the averaging-type collusion for the rest of this paper.

2.1. Motivation for group-based fingerprinting

One principle for enhancing the forensic capability of a multimedia fingerprinting system is to take advantage of any prior knowledge about potential collusion attacks during the design of the fingerprints. In this paper, we investigate mechanisms that improve the ability to identify colluders by exploiting fundamental properties of the collusion scenario. In particular, we observe that fingerprinting systems using orthogonal modulation do not consider the following issues.

(1) Orthogonal fingerprinting schemes are designed for the case where all users are equally likely to collude with each other. This assumption that users collude together in a uniformly random fashion is unreasonable. It is more reasonable that users from the same social or cultural background will collude together with a higher probability than with users from a different background. For example, a teenage user from Japan is more likely to collude with another teenager from Japan than with a middle-aged user from France. In general, the factors that lead to dividing the users into groups are up to the system designer to determine. Once the users have been grouped, we may take advantage of this grouping in a natural way: divide fingerprints into different subsets and assign each subset to a specific group whose members are more likely to collude with each other than with members from other groups.

(2) Orthogonality of fingerprints helps to distinguish individual users. However, this orthogonality also puts innocent users into suspicion with equal probability. It was shown in [16] that when the number of colluders

is beyond a certain value, catching one colluder successfully is very likely to require the detection system to suspect all users as guilty. This observation is obviously undesirable for any forensic system, and suggests that we introduce correlation between the fingerprints of certain users. In particular, we may introduce correlation between members of the same group, who are more likely to collude with each other. Therefore, when a specific user is involved in a collusion, users from the same group will be more likely accused than users from groups not containing colluders.

(3) The performance can be improved by applying appropriate detection strategies. The challenge is to take advantages of the previous points when designing the detection process.

By considering these issues, we can improve on the orthogonal fingerprinting system and provide a means to enhance collusion resistance. The underlying philosophy is to introduce a well-controlled amount of correlation into user fingerprints. Our fingerprinting systems involve two main directions of development: the development of classes of fingerprints capable of withstanding collusion and the development of forensic algorithms that can accurately and efficiently identify members of a colluding coalition. Therefore, for each of our proposed systems, we will address the issues of designing collusion-resistant fingerprints and developing efficient colluder detection schemes. To validate the improvement of such group-oriented fingerprinting system, we will evaluate the performance of our proposed systems under the average attack and compare the resulting collusion resistance to that of an orthogonal fingerprinting system.

3. TWO-TIER GROUP-ORIENTED FINGERPRINTING SYSTEM

3.1. Fingerprint design scheme

As an initial step for developing a group-oriented fingerprinting system, we present a two-tier scheme that consists of several groups, and within each group are users who are equally likely to collude with each other but less likely to collude with members from other groups. The design of our fingerprints are based upon: (1) grouping and (2) code modulation.

Grouping

The overall fingerprinting system is implemented by designing L groups. For simplicity, we assume that each group can accommodate up to M users. Therefore, the total number of users is $n = M \times L$. The choice of M is affected by many factors, such as the number of potential purchasers in a region and the collusion pattern of users. We also assume that fingerprints assigned to different groups are statistically independent of each other. There are two main advantages provided by independency between groups. First, the detection process is simple to carry out, and secondly, when collusion occurs, the independency between groups limits the amount of innocent users falsely placed under suspicion within a group, since the possibility of wrongly accusing another group is negligible.

Code modulation within each group

We will apply the same code matrix to each group. For each group i, there are v orthogonal basis signals $\mathbf{U}_i = [\mathbf{u}_{i1}, \mathbf{u}_{i2}, \ldots, \mathbf{u}_{iv}]$, each having Euclidean norm $\|\mathbf{u}\|$. We choose the sets of orthogonal bases for different groups to be independent. In code modulation, information is encoded into $\mathbf{s}_{ij}$, the jth fingerprint in group i, via

$$\mathbf{s}_{ij} = \sum_{l=1}^{v} c_{lj}\mathbf{u}_{il}, \tag{2}$$

where the symbol c_{lj} is a real value, and all $\mathbf{s}$ and $\mathbf{u}$ terms are column vectors with length N and equal energy. We define the *code matrix* $\mathbf{C} = (c_{lj}) = [\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_M]$ as the $v \times M$ matrix whose columns are the code vectors of different users. We have $\mathbf{S}_i = [\mathbf{s}_{i1}, \mathbf{s}_{i2}, \ldots, \mathbf{s}_{iM}] = \mathbf{UC}$, with the correlation matrix of $\{\mathbf{s}_{ij}\}$ as

$$\mathbf{R}_s = \|\mathbf{u}\|^2\mathbf{R}, \quad \mathbf{R} = \mathbf{C}^T\mathbf{C}. \tag{3}$$

The essential task in designing the set of fingerprints for each subsystem is to design the underlying correlation matrix $\mathbf{R}_s$. With the assumption in mind that the users in the same group are equally likely to collude with each other, we create the fingerprints in one group to have equal correlation. Thus, we choose a matrix $\mathbf{R}$ such that all its diagonal elements are 1 and all the off-diagonal elements are ρ. We will refer to ρ as the *intragroup correlation*.

For the proposed fingerprint design, we need to address such issues as the size of groups and the coefficient ρ. The parameters M and ρ will be chosen to yield good system performance. In our implementation, M is chosen to be the best supportable user size for the orthogonal modulation scheme [16]. In particular, when the total number of users is small, for instance $n \leq 100$, there is no advantage to having many groups, and it is sufficient to use one or two groups. As we will see later in (13), the detection performance for the single-group case is characterized by the mean difference $(1-\rho)\|\mathbf{s}\|/K$ for K colluders. A larger value of the mean difference is preferred, implying a negative ρ is favorable. On the other hand, when the fingerprinting system must accommodate a large number of users, there will be more groups and hence the primary task is to identify the groups containing colluders. In this case, a positive coefficient ρ should be employed to yield high accuracy in group detection. For the latter case, to simplify the detection process, we propose a structured design of fingerprints $\{\mathbf{s}_{ij}\}$'s, consisting of two components:

$$\mathbf{s}_{ij} = \sqrt{1-\rho}\,\mathbf{e}_{ij} + \sqrt{\rho}\,\mathbf{a}_i, \tag{4}$$

where $\{\mathbf{e}_{i1}, \ldots, \mathbf{e}_{iM}, \mathbf{a}_i\}$ are the orthogonal basis vectors of group i with equal energy. The bases of different groups are independent. It is easy to check the fact that $\mathbf{R}_s = N\sigma_u^2\mathbf{R}$ under this design scheme.

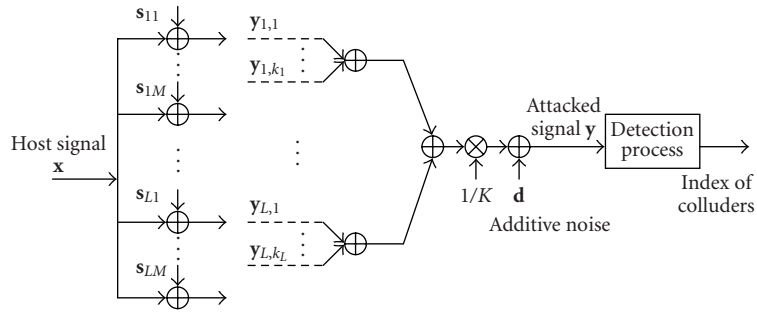


Figure 1: Model for collusion by averaging.

3.2. Detection scheme

The design of appropriate fingerprints must be complemented by the development of mechanisms that can capture those involved in the fraudulent use of content. When collusion occurs, the content owner's goal is to identify the fingerprints associated with users who participated in generating the colluded content. In this section, we discuss the problem of detecting the colluders when the above scheme is considered. In Figure 1, we depict a system accommodating n users, consisting of L groups with M users within each group. Suppose, when a collusion occurs involving K colluders who form a colluded content copy $\mathbf{y}$, that the number of colluders within group i is k_i and that k_i's satisfy $\sum_{i=1}^{L} k_i = K$. The observed content $\mathbf{y}$ after the average collusion is

$$\mathbf{y} = \frac{1}{K}\sum_{i=1}^{L}\sum_{j\in S_{ci}} \mathbf{y}_{ij} + \mathbf{d} = \frac{1}{K}\sum_{i=1}^{L}\sum_{j\in S_{ci}} \mathbf{s}_{ij} + \mathbf{x} + \mathbf{d}, \tag{5}$$

where $S_{ci} \subseteq [1,\ldots,M]$ indicates a subset of size $|S_{ci}| = k_i$ describing the members of group i that are involved in the collusion and the $\mathbf{s}_{ij}$'s are Gaussian distributed. We also assume that the additive distortion $\mathbf{d}$ is an N-dimensional vector following an i.i.d. Gaussian distribution with zero mean and variance σ_d^2. In this model, the number of colluders K and the subsets S_{ci}'s are unknown parameters. The nonblind scenario is assumed in our consideration, meaning that the host signal $\mathbf{x}$ is available at the detector and thus always subtracted from $\mathbf{y}$ for analysis.

The detection scheme consists of two stages. The first stage focuses on identifying groups containing colluders and the second one involves identifying colluders within each "guilty" group.

Stage 1—Group detection

Because of the independency of different groups and the assumption of i.i.d. Gaussian distortion, it suffices to consider the (normalized) correlator vector $\mathbf{T}_G$ for identifying groups possessing colluders. The ith component of $\mathbf{T}_G$ is expressed by

$$T_G(i) = \frac{(\mathbf{y}-\mathbf{x})^T(\mathbf{s}_{i1}+\mathbf{s}_{i2}+\cdots+\mathbf{s}_{iM})}{\sqrt{\|\mathbf{s}\|^2[M+(M^2-M)\rho]}} \tag{6}$$

for $i = 1,2,\ldots,L$. Utilizing the special structure of the correlation matrix $\mathbf{R}_s$, we can show that the distribution follows

$$p(T_G(i)\,|\,K,k_i,\sigma_d^2) = \begin{cases} N(0,\sigma_d^2), & \text{if } k_i = 0, \\ N\left(\dfrac{k_i\|\mathbf{s}\|\sqrt{1+(M-1)\rho}}{K\sqrt{M}}, \sigma_d^2\right), & \text{otherwise,} \end{cases} \tag{7}$$

where $k_i = 0$ indicates that no user within group i is involved in the collusion attack. We note that based on the independence of fingerprints from different groups, the $T_G(i)$ are independent of each other. Further, based on the distribution of $T_G(i)$, we see that if no colluder is present in group i, $T_G(i)$ will only consist of small contributions. However, as the amount of colluders belonging to group i increases, we are more likely to get a larger value of $T_G(i)$.

We employ the correlators $T_G(i)$'s for detecting the presence of colluders within each group. For each i, we compare $T_G(i)$ to a threshold h_G and report that the ith group is *colluder present* if $T_G(i)$ exceeds h_G. That is,

$$\hat{\mathbf{i}} = \arg_{i=1}^{L}\{T_G(i) \geq h_G\}, \tag{8}$$

where the set $\hat{\mathbf{i}}$ indicates the indices of groups including colluders. As indicated in the distribution (7), the threshold h_G here is determined by the pdf. Since normally the number of groups involved in the collusion is small, we can correctly classify groups with high probability under the nonblind scenario.

Stage 2—Colluder detection within each group

After classifying groups into the colluder-absent class or the colluder-present class, we need to further identify colluders within each group. For each group $i \in \hat{\mathbf{i}}$, because of the orthogonality of basis $[\mathbf{u}_{i1},\mathbf{u}_{i2},\ldots,\mathbf{u}_{iM}]$, it is sufficient to consider the correlators $\mathbf{T}_i$, with the jth component $T_i(j) = (\mathbf{y}-\mathbf{x})^T\mathbf{u}_{ij}/\sqrt{\|\mathbf{u}\|^2}$ for $j = 1,\ldots,M$. We can show that

$$\mathbf{T}_i = \frac{\|\mathbf{u}\|}{K}\mathbf{C}\boldsymbol{\Phi}_i + \mathbf{n}_i, \tag{9}$$

where $\boldsymbol{\Phi} \in \{0,1\}^M$ with $\Phi_i(j) = 1$ for $j \in S_{ci}$, indicates colluders within group i via the location of components whose

values are 1; and $\mathbf{n}_i = \mathbf{U}_i\mathbf{d}^T/\sqrt{\|\mathbf{u}\|^2}$, follows an $N(0,\sigma_d^2\mathbf{I}_M)$ distribution. Thus, we have the distribution

$$p(\mathbf{T}_i\,|\,K,S_{ci},\sigma_d^2) = N\left(\frac{\|\mathbf{u}\|}{K}\mathbf{C}\boldsymbol{\Phi}_i,\sigma_d^2\mathbf{I}_M\right). \tag{10}$$

Suppose the parameters K and k_i are assumed known, we can estimate the subset S_{ci} via

$$\begin{aligned}\hat{S}_{ci} &= \arg\max_{|S_{ci}|=k_i} p(\mathbf{T}_i|K,S_{ci},\sigma_d^2)\\ &= \text{the indices of } k_i \text{ largest } T_{si}(j)\text{'s},\end{aligned} \tag{11}$$

where the jth component of the correlator vector $\mathbf{T}_{si}$ is defined as

$$T_{si}(j) = \mathbf{T}_i^T\mathbf{c}_j = \frac{(\mathbf{y}-\mathbf{x})^T\mathbf{s}_{ij}}{\sqrt{\|\mathbf{s}\|^2}} \tag{12}$$

and $\mathbf{T}_{si}$ has the distribution

$$\begin{aligned}&p(\mathbf{T}_{si}\,|\,K,S_{ci},\sigma_d^2) = N(\boldsymbol{\mu}_i,\sigma_d^2\mathbf{R}),\\ &\text{where } \mu_i(j) = \begin{cases}\dfrac{1+(k_i-1)\rho}{K}\|\mathbf{s}\|, & \text{if } j\in S_{ci},\\ \dfrac{k_i\rho}{K}\|\mathbf{s}\|, & \text{otherwise.}\end{cases}\end{aligned} \tag{13}$$

The derivation of (11) and (13) can be found in Appendix A. However, applying (11) to locate colluders within group i is not preferred in our situation for two reasons. First, knowledge of K and k_i are usually not available in practice and must be estimated. Further, the above approach aims to minimize the joint estimation error of all colluders and it lacks the capability of adjusting parameters for addressing specific system design goals, such as minimizing the probability of a false positive and maximizing the probability of catching at least one colluder. Regardless of these concerns, the observation in (11) suggests the use of $\mathbf{T}_{si}$ for colluder detection within each group.

To overcome the limitations of the detector in (11), we employ a colluder identification approach within each group $i\in\hat{\mathbf{i}}$ by comparing the correlator $T_{si}(j)$ to a threshold h_i and indicating a colluder presence whenever $T_{si}(j)$ is greater than the threshold. That is,

$$\hat{\mathbf{j}}_i = \arg_{j=1}^{M}\{\mathbf{T}_{si}(j)\geq h_i\}, \tag{14}$$

where the set $\hat{\mathbf{j}}_i$ indicates the indices of colluders within group i, and the threshold h_i is determined by other parameters and the system requirements.

In our approach, we choose the thresholds such that false alarm probabilities satisfy

$$\begin{aligned}\Pr\{T_G(i)\geq h_G \mid k_i=0\} &= Q\left(\frac{h_G}{\sigma_d}\right) = \alpha_1,\\ \Pr\{T_{si}(j)\geq h_i \mid k_i,\ j\notin S_{ci}\} &= Q\left(\frac{h_i - k_i\rho\|s\|/K}{\sigma_d}\right) = \alpha_2,\end{aligned} \tag{15}$$

where the Q-function is $Q(t) = \int_t^\infty(1/\sqrt{2\pi})\exp(-x^2/2)dx$, and the values of α_1 and α_2 depend upon the system requirements.

When the fingerprint design scheme in (4) is applied to accommodate a large number of users, we observe the following:

$$\begin{aligned}T_{si}(j) &= \frac{(\mathbf{y}-\mathbf{x})^T\mathbf{s}_{ij}}{\sqrt{\|\mathbf{s}\|^2}} = T_{ei}(j)+T_a(i),\\ T_{ei}(j) &= \frac{\sqrt{1-\rho}(\mathbf{y}-\mathbf{x})^T\mathbf{e}_{ij}}{\sqrt{\|\mathbf{s}\|^2}},\\ T_a(i) &= \frac{\sqrt{\rho}(\mathbf{y}-\mathbf{x})^T\mathbf{a}_i}{\sqrt{\|\mathbf{s}\|^2}},\end{aligned} \tag{16}$$

thus

$$\begin{aligned}&p(\mathbf{T}_{ei}\,|\,K,S_{ci},\sigma_d^2) = N(\boldsymbol{\mu}_{ei},(1-\rho)\sigma_d^2\mathbf{I}_M),\\ &\text{with } \mu_{ei}(j) = \begin{cases}\dfrac{1-\rho}{K}\|\mathbf{s}\|, & \text{if } j\in S_{ci},\\ 0, & \text{otherwise,}\end{cases}\\ &p(T_a(i)\,|\,K,S_{ci},\sigma_d^2) = N(k_i\rho\|\mathbf{s}\|/K,\rho\sigma_d^2).\end{aligned} \tag{17}$$

Since, for each group i, $T_a(i)$ is common for all $T_{si}(j)$'s, it is only useful in group detection and can be subtracted in detecting colluders. Therefore, the detection process (14) in stage 2 now becomes

$$\hat{\mathbf{j}}_i = \arg_{j=1}^{M}\{\mathbf{T}_{ei}(j)\geq h\}. \tag{18}$$

Now the threshold h is chosen such that

$$\begin{aligned}&\Pr\{T_{ei}(j)\geq h \mid j\notin S_{ci}\}\\ &\quad= Q\left(\frac{h}{\sigma_d\sqrt{1-\rho}}\right) = \alpha_2, \quad \text{thus } h = Q^{-1}(\alpha_2)\sigma_d\sqrt{1-\rho}.\end{aligned} \tag{19}$$

Note that h is a common threshold for different groups. Advantages of the process (18) are that components of the vector $\mathbf{T}_{ei}$ are independent and that the resulting variance is smaller than σ_d^2.

3.3. Performance analysis

One important purpose of a multimedia fingerprinting system is to trace the individuals involved in digital content fraud and provide evidence to both the company administering the rights associated with the content and law enforcement agencies. In this section, we show the performance of the above fingerprinting system under different performance criteria. To compare with the orthogonal scheme [16], we assume the overall MSE with respect to the host signal is constant. More specifically,

$$E\{\|\mathbf{y}-\mathbf{x}\|^2\} = \left(\frac{1-\rho}{K}+\frac{\rho\sum_{i=1}^{L}k_i^2}{K^2}\right)\|\mathbf{s}\|^2 + N\sigma_d^2 \triangleq \|\mathbf{s}\|^2, \tag{20}$$

meaning the overall MSE equals the fingerprint energy. Therefore, the variance σ_d^2 is based on $\{k_i\}$ correspondingly.

Different concerns arise in different fingerprinting applications. In studying the effectiveness of a detection algorithm in collusion applications, there are several performance criteria that may be considered. For instance, one popular set of performance criteria involves measuring the probability of a false negative (miss) and the probability of a false positive (false alarm) [12, 13]. Such performance metrics are significant when presenting forensic evidence in a court of law, since it is important to quantify the reliability of the evidence when claiming an individual's guilt. On the other hand, ifthe overall system security is a major concern, the goal would then be to quantify the likelihood of catching *all* colluders, since missed detection of any colluder may result in severe consequences. Further, multimedia fingerprinting may aim to provide evidence *supporting* the suspicion of a party. Tracing colluders via fingerprints should work in concert with other operations. For example, when a user is considered as a suspect based on multimedia forensic analysis, the agencies enforcing the digital rights can more closely monitor that user and gather additional evidence that can be used collectively for *proving* the user's guilt. Overall, identifying colluders through anticollusion fingerprinting is one important component of the whole forensic system, and it is the confidence in the fidelity of all evidence that allows a colluder to be finally identified and their guilt sustained in court. This perspective suggests that researchers consider a broad spectrum of performance criteria for forensic applications. We therefore consider the following three sets of performance criteria. Without loss of generality, we assume $\mathbf{i} = [1, 2, \ldots, l]$, where $\mathbf{i}$ indicates the indices of groups containing colluders and l is the number of groups containing colluders.

3.3.1. Case 1 (catch at least one colluder)

One of the most popular criteria explored by researchers are the probability of a false negative (P_{fn}) and the probability of a false positive (P_{fp}) [12, 13]. The major concern is to identify at least one colluder with high confidence without accusing innocent users. From the detector's point of view, a detection approach fails if either the detector fails to identify any of the colluders (a false negative) or the detector falsely indicates that an innocent user is a colluder (a false positive). We first define a false alarm event A_i and a correct detection event B_i for each group i,

$$\begin{aligned} A_i &= \left\{ T_G(i) \geq h_G, \max_{j \notin S_{ci}} T_{si}(j) \geq h_i \right\}; \\ B_i &= \left\{ T_G(i) \geq h_G, \max_{j \in S_{ci}} T_{si}(j) \geq h_i \right\} \end{aligned} \tag{21}$$

for the scheme of (14), or

$$\begin{aligned} A_i &= \left\{ T_G(i) \geq h_G, \max_{j \notin S_{ci}} T_{ei}(j) \geq h \right\}; \\ B_i &= \left\{ T_G(i) \geq h_G, \max_{j \in S_{ci}} T_{ei}(j) \geq h \right\} \end{aligned} \tag{22}$$

for the scheme of (18). Then we have

$$\begin{aligned} P_d &= \Pr\left\{ \exists \hat{\mathbf{j}}_i \cap S_{ci} \neq \varnothing \right\} = \Pr\left\{ \cup_{i=1}^{l} B_i \right\}, \\ &= \Pr\{B_1\} + \Pr\{\bar{B}_1 \cap B_2\} \\ &\quad + \cdots + \Pr\{\bar{B}_1 \cap \bar{B}_2 \cdots \cap \bar{B}_{l-1} \cap B_l\} \\ &= \sum_{i=1}^{l} q_i \Pi_{j=1}^{i-1} (1 - q_j), \quad q_i = \Pr\{B_i\}, \\ P_{fp} &= \Pr\left\{ \exists \hat{\mathbf{j}}_i \cap \bar{S}_{ci} \neq \varnothing \right\} = \Pr\left\{ \cup_{i=1}^{L} A_i \right\} \\ &= \Pr\left\{ \cup_{i \notin \mathbf{i}} A_i \right\} + \left(1 - \Pr\left\{ \cup_{i \notin \mathbf{i}} A_i \right\}\right) \Pr\left\{ \cup_{i=1}^{l} A_i \right\} \\ &= \left[1 - (1 - p_{l+1})^{L-l} \right] + (1 - \alpha_1)^{L-l} \Pr\left\{ \cup_{i=1}^{l} A_i \right\} \\ &= \left[1 - (1 - p_{l+1})^{L-l} \right] \\ &\quad + (1 - p_{l+1})^{L-l} \sum_{i=1}^{l} p_i \Pi_{j=1}^{i-1} (1 - p_j), \quad p_i = \Pr\{A_i\}. \end{aligned} \tag{23}$$

These formulas can be derived by utilizing the law of total probability in conjunction with the independency between fingerprints belonging to different groups and the fact that $p_{l+1} = p_{l+2} = \cdots = p_L$ since there are no colluders in $\{A_{l+1}, \ldots, A_L\}$. Based on this pair of criteria, the system requirements are represented as

$$P_{fp} \leq \epsilon; \qquad P_d \geq \beta. \tag{24}$$

We can see that the difficulty in analyzing the collusion resistance lies in calculating joint probabilities p_i's and q_i's. When the total number of users is small such that all the users will belong to one or two groups, stage 1 (guilty group identification) is normally unnecessary and thus ρ should be chosen to maximize the detection probability in stage 2. We note that the detection performance is characterized by the difference between the means of the two hypotheses in (13) and hence is given by $(1 - \rho)\|\mathbf{s}\|/K$. Therefore, a negative ρ is preferred. Since the matrix $\mathbf{R}$ should be positive definite, $1 + (M - 1)\rho > 0$ is required. We show the performance by examples when the total number of users is small, as in Figure 2a, where $n = 100$, $M = 50$, and a negative $\rho = -0.01$ is used. It is clear that introducing a negative ρ helps to improve the performance when n is small. It also reveals that the worst case in performance happens when each guilty group contributes equal number of colluders, meaning $k_i = K/|\mathbf{i}|$, for $i \in \mathbf{i}$.

In most applications, however, the total number of users n is large. Therefore, we focus on this situation for performance analysis. One approach to accommodate large n is to design the fingerprints according to (4) and use a positive value of ρ. Now after applying the detection scheme in (18), the events A_i's and B_i's are defined as in (22). We further note, referring to (6), (16), and (17), that the correlation coefficient between $T_G(i)$ and $T_{ei}(j)$ is equal to $\sqrt{(1 - \rho)/(M + (M^2 - M)\rho)}$, which is a small value close to 0. For instance, with $\rho = 0.2$ and $M = 60$, this correlation coefficient is as small as 0.03. This observation suggests that

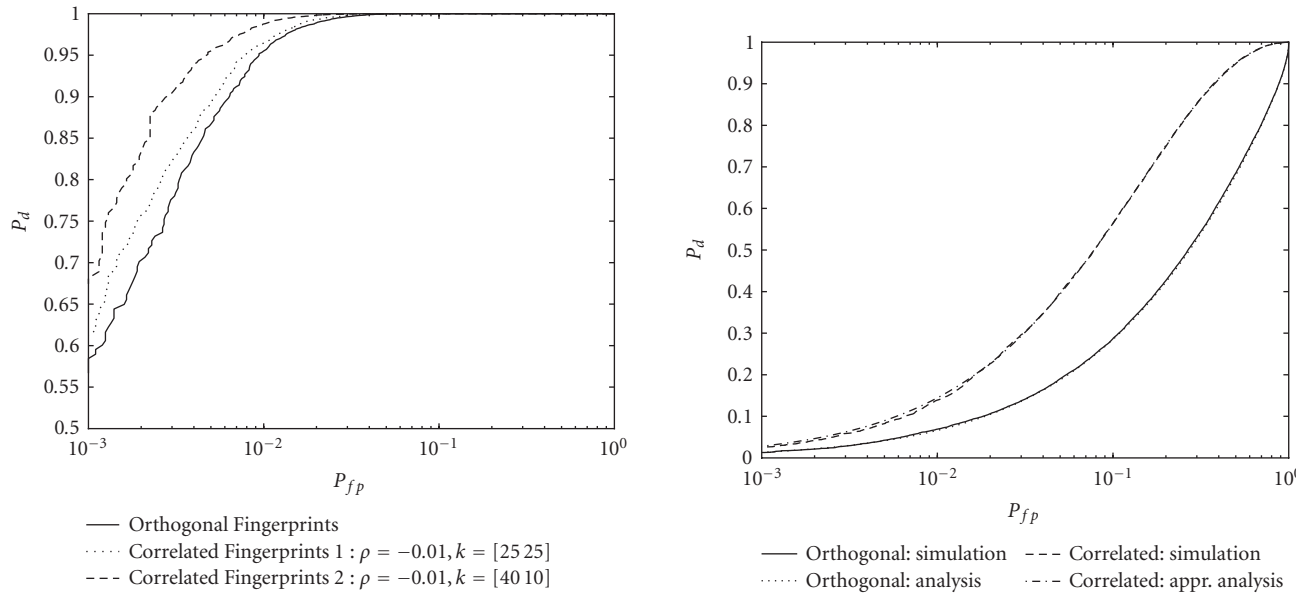


FIGURE 2: ROC curves P_d versus P_{fp} of different examples, compared with the orthogonal scheme in [16], with $N = 10^4$. In (a), a small number of users $n = 100$ and a negative $\rho = -0.01$ are considered. We have $M = 50$ and $K = 50$. In (b), a large number of users $n = 6000$ and a positive $\rho = 0.4$ are considered where $M = 60, \alpha_1 = 10^{-6}$, and eight groups involve in collusion with each group having eight colluders.

$T_G(i)$ and $T_{ei}(j)$'s are approximately uncorrelated, therefore we have the following approximations in calculating P_{fp} and P_d in (24):

$$\begin{aligned} p_i &\approx \Pr\{T_G(i) \geq h_G\} \Pr\left\{\max_{j \notin S_{ci}} T_{ei}(j) \geq h\right\} \\ &= Q\left(\frac{h_G - k_i r_0}{\sigma_d}\right)\left[1 - \left(1 - Q\left(\frac{h}{\sigma_d\sqrt{1-\rho}}\right)\right)^{M-k_i}\right], \\ q_i &\approx \Pr\{T_G(i) \geq h_G\} \Pr\left\{\max_{j \in S_{ci}} T_{ei}(j) \geq h\right\} \\ &= Q\left(\frac{h_G - k_i r_0}{\sigma_d}\right)\left[1 - \left(1 - Q\left(\frac{h - (1-\rho)\|\mathbf{s}\|/K}{\sqrt{1-\rho}\sigma_d}\right)\right)^{k_i}\right] \end{aligned} \tag{25}$$

with $r_0 = \|\mathbf{s}\|\sqrt{1 + (M-1)\rho}/K\sqrt{M}$. Note that here we employ the theory of order statistics [24]. We show an example in Figure 2b, where $n = 6000$, $L = 100$, and there are eight groups involved in collusion with each group having eight colluders. We note that this approximation is very accurate compared to the simulation result, and that our fingerprinting scheme is superior to using orthogonal fingerprints.

To have an overall understanding of the collusion resistance of the proposed scheme, we further study the maximum resistible number of colluders $K_{\max}$ as a function of n. For a given n, M, and $\{k_i\}$'s, we choose the parameters α_1, which determines the threshold h_G, α_2, which determines the threshold h, and ρ, which determines the probability of the group detection, so that

$$\begin{aligned} &\{\alpha_1, \alpha_2, \rho\} \\ &\quad = \arg \max_{\{\alpha_1,\alpha_2,\rho\}} P_d(\alpha_1, \alpha_2, \rho) \quad \text{subject to } P_{fp}(\alpha_1, \alpha_2, \rho) \leq \epsilon. \end{aligned} \tag{26}$$

In reality, the value of ρ is limited by the quantization precision of the image system and ρ should be chosen at the fingerprint design stage. Therefore, ρ is fixed in real applications. Since, in many collusion scenarios the size $|\mathbf{i}|$ would be reasonably small, our results are not as sensitive to α_1 and ρ as to α_2, and the group detection in stage 1 often yields very high accuracy. For example, when $|\mathbf{i}| \leq 5$, the threshold h_G can be chosen such that $\alpha_1 \ll \epsilon$ and $\Pr(T_G(i) \geq h_G)$ is sufficiently close to 1 for at least one group $i \in \mathbf{i}$. Therefore, to simplify our searching process, we can fix the values of α_1. Also, in the design stage, we consider the performance of the worst case, where $k_i = K/|\mathbf{i}|$, for $i \in \mathbf{i}$. One important efficiency measure of a fingerprinting scheme is $K_{\max}$, the maximum number of colluders that can be tolerated by a fingerprinting system such that the system requirements are still satisfied. We illustrate an example in Figure 3, where $M = 60$ is used since it is shown to be the best supportable user size for the orthogonal scheme [16], and the number of guilty groups is up to five. It is noted that $K_{\max}$ of the proposed scheme (indicated by the dotted and the dashed-dotted lines) is larger than that of the orthogonal scheme (the solid line) when n is large. The difference between the lower bound and upper bound is due to the fact that $k_i = K/|\mathbf{i}|$ in our simulations.

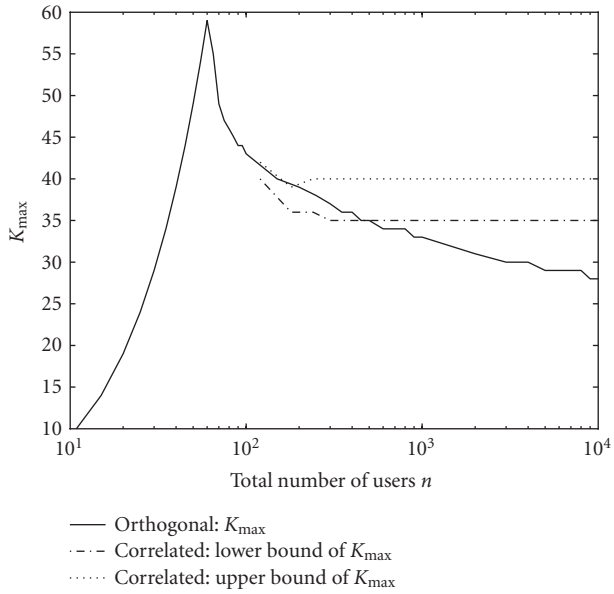


Figure 3: Comparison of collusion resistance of the orthogonal and the proposed group-based fingerprinting systems to the average attack. Here, $N = 10^4$, $M = 60$, $k_i = K/|i|$, $|i| = 5$, and the system requirements are represented by $\epsilon = 10^{-3}$ and $\beta = 0.8$.

Overall, the group-oriented fingerprinting system provides the performance improvement by yielding better collusion resistance. It is worth mentioning that the performance is fundamentally affected by the collusion pattern. The smaller the number of guilty groups, the better chance the colluders are identified.

3.3.2. Case 2 (fraction of guilty captured versus fraction of innocent accused)

This set of performance criteria consists of the expected fraction of colluders that are successfully captured, denoted as r_c, and the expected fraction of innocent users that are falsely placed under suspicion, denoted as r_i. Here, the major concern is to catch more colluders, possibly at a cost of accusing more innocents. The balance between capturing colluders and placing innocents under suspicion is represented by these two expected fractions. Suppose the total number of users n is large, and the detection scheme in (18) is applied. We have

$$\begin{aligned} r_i &= \frac{E\left(\sum_{i=1}^{l}\sum_{j\notin S_{ci}}\gamma_{ij}+\sum_{i=l+1}^{L}\sum_{j=1}^{M}\gamma_{ij}\right)}{n-K} \\ &= \frac{\sum_{i=1}^{l}(M-k_i)p_{0i}+M(L-l)p_{0,l+1}}{n-K}, \\ r_c &= \frac{E\left(\sum_{i=1}^{l}\sum_{j\in S_{ci}}\gamma_{ij}\right)}{K} = \frac{\sum_{i=1}^{l}k_i p_{1i}}{K}, \end{aligned} \tag{27}$$

where

$$\begin{aligned} p_{1i} &= \Pr\{T_G(i)\geq h_G, T_{ei}(j)\geq h_i \mid j\in S_{ci}\}, \quad \text{for } i=1,\ldots,l, \\ p_{0i} &= P_r\{T_G(i)\geq h_G, T_{ei}(j)\geq h_i \mid j\notin S_{ci}\}, \quad \text{for } i=1,\ldots,l+1, \end{aligned} \tag{28}$$

and γ_{ij} is defined as

$$\gamma_{ij} = \begin{cases} 1, & \text{if } j\text{th user of group } i \text{ is accused,} \\ 0, & \text{otherwise.} \end{cases} \tag{29}$$

Based on this pair $\{r_i, r_c\}$, the system requirements are represented by

$$r_i \leq \alpha_i; \qquad r_c \geq \alpha_c. \tag{30}$$

We further notice that $T_G(i)$ and $T_{ei}(j)$'s are approximately uncorrelated, therefore, we can approximately apply $p_{1i} = P_r\{T_G(i)\geq h_G\}P_r\{T_{ei}(j)\geq h \mid j\in S_{ci}\}$, for $i = 1,\ldots,l$, and $p_{0i} = P_r\{T_G(i)\geq h_G\}P_r\{T_{ei}(j)\geq h \mid j\notin S_{ci}\}$, for $i = 1,\ldots,l+1$ in calculating r_i and r_c. With a given n, M, and $\{k_i\}$'s, the parameters α_1 which determines the threshold h_G, α_2 which determines the threshold h, and ρ which determines the probability of the group detection, are chosen such that

$$\max_{\{\alpha_1,\alpha_2,\rho\}} r_c(\alpha_1,\alpha_2,\rho) \quad \text{subject to } r_i(\alpha_1,\alpha_2,\rho)\leq\alpha_i. \tag{31}$$

Similarly, finite discrete values of α_1 and ρ are considered to reduce the computational complexity.

We first illustrate the resistance performance of the system by an example, shown in Figure 4a, where $N = 10^4$, $\rho = 0.2$, and three groups involved in collusion with each group including 15 colluders. We note that the proposed scheme is superior to using orthogonal fingerprints. In particular, for the proposed scheme, all colluders are identified as long as we allow 10 percent innocents to be wrongly accused. We further examine $K_{\max}$ for the case that $k_i = K/|\mathbf{i}|$ when different number of users is managed, as shown in Figure 4b by requiring $r \leq 0.01$ and $P_d \geq 0.5$ and setting $M = 60$ and the number of guilty groups is up to ten. The $K_{\max}$ of our proposed scheme is larger than that of $K_{\max}$ for orthogonal fingerprinting when large n is considered.

3.3.3. Case 3 (catch all colluders)

This set of performance criteria consists of the efficiency rate r, which describes the amount of expected innocents accused per colluder, and the probability of capturing all K colluders, which we denote by P_d. The goal in this scenario is to capture all colluders with a high probability. The tradeoff between capturing colluders and placing innocents under suspicion is achieved through the adjustment of the efficiency rate r. More specifically, suppose n is large and the detection scheme in (18) is applied, we have

$$\begin{aligned} r &= \frac{E\left(\sum_{i=1}^{l}\sum_{j\notin S_{ci}}\gamma_{ij}+\sum_{i=l+1}^{L}\sum_{j=1}^{M}\gamma_{ij}\right)}{E\left(\sum_{i=1}^{l}\sum_{j\in S_{ci}}\gamma_{ij}\right)} \\ &= \frac{\sum_{i=1}^{l}(M-k_i)p_{0i}+M(L-l)p_{0,l+1}}{\sum_{i=1}^{l}k_i p_{1i}}, \\ P_d &= P_r\{\forall S_{ci}\subseteq\hat{\mathbf{j}}_i\} \\ &= \Pi_{i=1}^{l}P_r\{C_i\}, \quad \text{with } C_i = \{T_G(i)\geq h_G, \min_{j\in S_{ci}} T_{ei}(j)\geq h\}, \end{aligned} \tag{32}$$

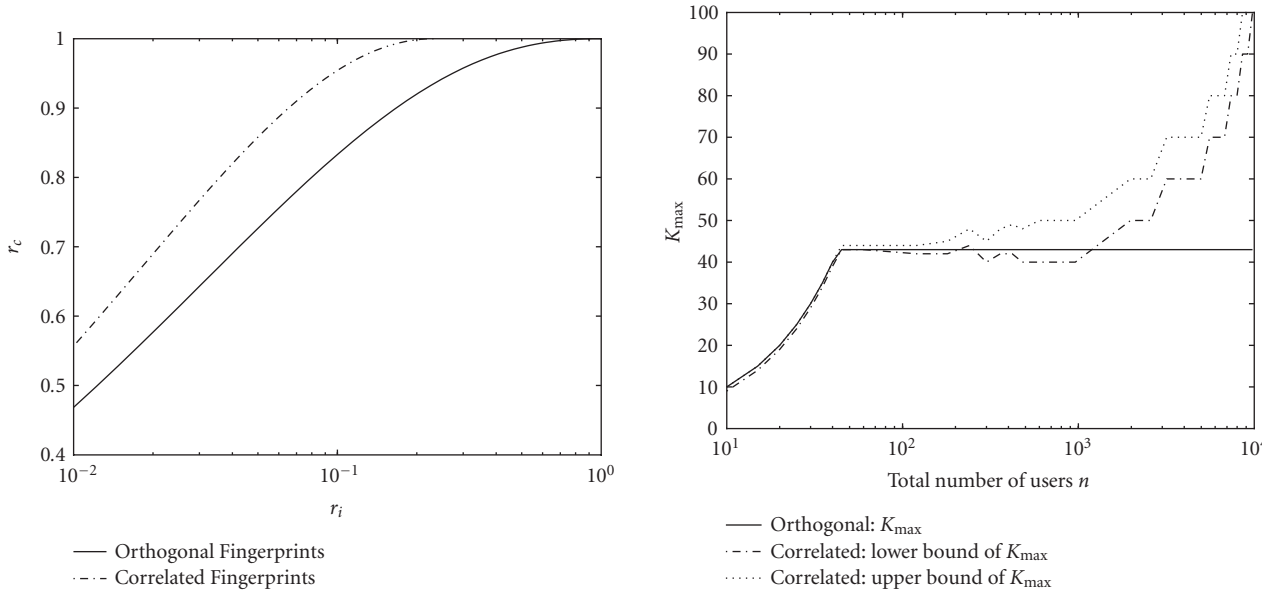


FIGURE 4: The resistance performance of the group-oriented and the orthogonal fingerprinting system under the criteria r_i and r_c. Here, $N = 10^4$. In (a), we have $M = 50$, $n = 500$, $\rho = 0.2$; $K_{\max}$ versus n is plotted in (b), where $M = 60$, the number of colluders within guilty groups are equal, meaning $k_i = K/|\mathbf{i}|$, the number of guilty groups is $|\mathbf{i}| = 10$, and the system requirements are represented by $\alpha = 0.01$ and $\beta = 0.5$.

in which p_{0i} and p_{1i} are defined as in (27). Based on this pair $\{r, P_d\}$, the system requirements are expressed as

$$r \le \alpha; \qquad P_d \ge \beta. \tag{33}$$

Similar to the previous cases, we further notice that $T_G(i)$ and $T_{ei}(j)$'s are approximately uncorrelated, and we may approximately calculate p_{1i}'s and p_{0i}'s as done earlier. Using the independency, we also apply the approximation

$$\begin{aligned} P_r\{C_i\} &= P_r\{T_G(i) \ge h_G\} P_r\left\{\min_{j\in S_{ci}} T_{ei}(j) \ge h\right\} \\ &= Q\left(\frac{h_G - k_i r_0}{\sigma_d}\right) Q\left(\frac{h - (1-\rho)\|\mathbf{s}\|}{\sigma_d\sqrt{1-\rho}}\right)^{k_i} \end{aligned} \tag{34}$$

in calculating P_d. With a given n, M, and $\{k_i\}$'s, the parameters α_1 which determines the threshold h_G, α_2 which determines the threshold h, and ρ which determines the probability of the group detection, are chosen such that

$$\max_{\{\alpha_1,\alpha_2,\rho\}} P_d(\alpha_1, \alpha_2, \rho) \quad \text{subject to } r(\alpha_1, \alpha_2, \rho) \le \alpha. \tag{35}$$

Similarly, finite discrete values of α_1 and ρ are considered to reduce the computational complexity.

We illustrate the resistance performance of the proposed system by two examples shown in Figure 5. It is worth mentioning that the accuracy in the group detection stage is critical for this set of criteria, since a miss-detection in stage 1 will result in a much smaller P_d. When capturing all colluders with high probability is a major concern, our proposed group-oriented scheme may not be favorable in cases where there are a moderate number of guilty groups involved in collusion or when the collusion pattern is highly asymmetric. The reason is that, under these situations, a threshold in stage 1 should be low enough to identify all colluder-present groups, however, a low threshold also results in wrongly accusing innocent groups. Therefore, stage 1 is not very useful in these situations.

4. TREE STRUCTURE-BASED FINGERPRINTING SYSTEM

In this section, we propose to extend our construction to represent the natural social and geographic hierarchical relationships between users by generalizing the two-tier approach to a more flexible group-oriented fingerprinting system based on a tree structure. As in the two-tier group-oriented system, to validate the improvement of such tree-based group fingerprinting, we will evaluate the performance of our proposed system under the average attack and compare the resulting collusion resistance to that of an orthogonal fingerprinting system.

4.1. *Fingerprint design scheme*

The group-oriented system proposed earlier can be viewed as a symmetric two-level tree-structured scheme. The first level consists of L nodes, with each node supporting P leaves that correspond to the fingerprints of individual users within one group. We observe that a user is often more likely to

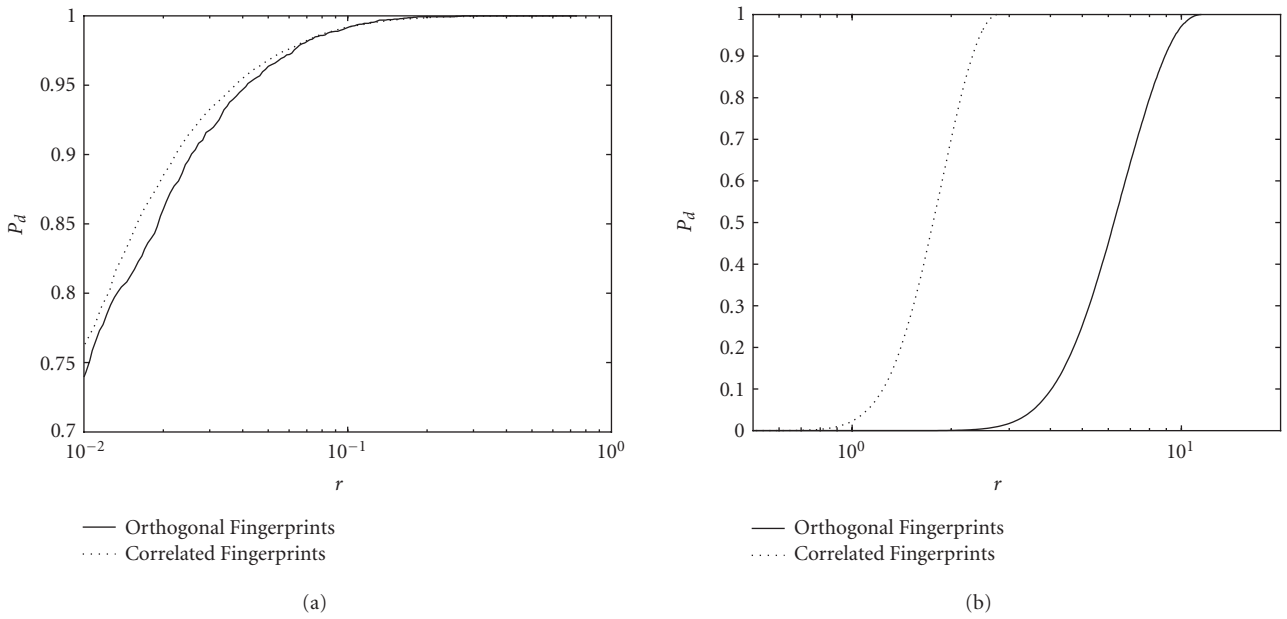


Figure 5: Performance curves P_d versus r of different examples, compared with the orthogonal scheme in [16]. Here $N = 10^4$. In (a), $K = 23$, a small number of users $n = 40$ and a negative $\rho = -0.023$ are considered. In (b), $M = 60$, a large number of users $n = 600$ and a positive $\rho = 0.3$ are considered. Three groups are involved in collusion, with numbers of colluders are $[32, 8, 8]$, respectively.

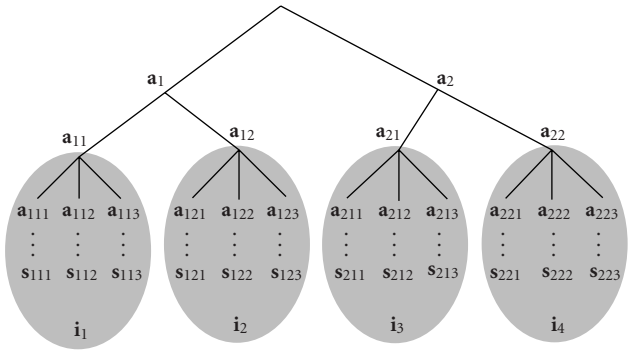


Figure 6: A tree structure-based fingerprinting scheme.

collude with some groups than with other groups. If we allow for a more general tree structure in the fingerprint design, we can achieve more flexibility in capturing the collusion dynamics between different groups. For instance, we may consider a simple region-based collusion pattern: users within Maryland are more likely to come together in generating an attacked copy than they are likely to collude with other users from Texas, and the probability for these two groups to come together to collude is higher than they would with users from Asia. We may view this subgroup hierarchy via a tree structure, as depicted in Figure 6. In this diagram, we assume that (1) users in region $\mathbf{i}_1$ are equally likely to collude with each other with a probability p_1 and (2) each user in region $\mathbf{i}_1$ is equally likely to collude with users within region $\mathbf{i}_2$ with a probability p_2 and users within other regions corresponding to different subtrees with a probability p_3, where $p_1 > p_2 > p_3$. Therefore, it is desirable for us to design a fingerprint tree that matches the large-scale collusion pattern (e.g., represented by the cultural, social, and geographic relationships among users) in such a way that the fingerprints on the same branch of the tree are more correlated with each other than with those on other branches, and correspondingly the associated users on the same branch of the tree are more likely to collude with each other.

More generally, we design a tree with M levels where each node at the $(m-1)$th level supports a total of L_m nodes. Let $[i_1, \ldots, i_M]$ indicate the index vector of a user/fingerprint. Exploiting the tree structure, we propose the following design of fingerprints $\{\mathbf{s}_{i_1,\ldots,i_M}\}$:

$$\mathbf{s}_{i_1,\ldots,i_M} = \sqrt{\rho_1}\mathbf{a}_{i_1} + \cdots + \sqrt{\rho_{M-1}}\mathbf{a}_{i_1,\ldots,i_{M-1}} + \sqrt{1 - \sum_{j=1}^{M-1} \rho_j}\,\mathbf{a}_{i_1,\ldots,i_M}, \tag{36}$$

where the $\mathbf{a}$ vectors correspond to orthogonal basis vectors with equal energy $\|\mathbf{a}\| = \|\mathbf{s}\|$, each ρ_j satisfies $0 \le \rho_j \le 1$, and $\rho_M = 1 - \sum_{j=1}^{M-1} \rho_j$. In this design scheme, the correlations between fingerprints are controlled by adjusting the coefficients ρ_i's, which are determined by the probabilities for users under different tree branches to carry out collusion attacks.

4.2. Detection scheme

We now discuss the problem of detecting the colluders when the proposed fingerprint design scheme in (36) is employed. For simplicity in analysis, we consider a balanced tree structure, where the system accommodates n users, and the tree involves M levels where each node at the $(m-1)$th level supports L_m nodes. The marked copy for a user with the index

vector $[i_1,\ldots,i_M]$ is represented as $\mathbf{y}_{i_1,\ldots,i_M}=\mathbf{x}+\mathbf{s}_{i_1,\ldots,i_M}$, where $\mathbf{x}$ is the host signal. When a collusion occurs, suppose that a total of K colluders are involved in forming a copy of colluded content $\mathbf{y}$, and the number of colluders within each level m subregion represented by an index vector $[i_1,\ldots,i_m]$ is $k_{i_1,\ldots,i_m}$. For instance, for a tree with $M=3$, in a subregion where users are all with indices $i_1=2$ and $i_2=1$, if $\mathbf{s}_{2,1,1}$ and $\mathbf{s}_{2,1,3}$ are colluders, then $k_{2,1}=2$. We note that, for each level $m=1,\ldots,M$, we have $\sum_{i_1=1}^{L_1}\cdots\sum_{i_m=1}^{L_m}k_{i_1,\ldots,i_m}=K$. The observed content $\mathbf{y}$ after the average collusion is

$$\mathbf{y}=\frac{1}{K}\sum_{\mathbf{i}_c\in\mathbf{S}_c}\mathbf{y}_{\mathbf{i}_c}+\mathbf{d}=\frac{1}{K}\sum_{\mathbf{i}_c\in\mathbf{S}_c}\mathbf{s}_{\mathbf{i}_c}+\mathbf{x}+\mathbf{d}, \tag{37}$$

where $\mathbf{i}_c$ indicates the index vector of length M, $\mathbf{S}_c$ indicates a vector set of size K, and each element of $\mathbf{S}_c$ is an index vector. We also assume that additional noise $\mathbf{d}$ is introduced after the average collusion and $\mathbf{d}$ is a vector following an i.i.d. Gaussian distribution with zero mean and variance σ_d^2. The number of colluders K and the set $\mathbf{S}_c$ are the parameters to be estimated. We consider the nonblind scenario, where the host signal $\mathbf{x}$ is available at the detector and thus always subtracted from $\mathbf{y}$ for analysis.

Using such a formulation, we will address the issue of detecting the colluders. The tree-structured, hierarchical nature of group-oriented fingerprints leads to a *multistage* colluder identification scheme: the first stage focuses on identifying the "guilty" regions at the first level; at the second stage, we further narrow down by specifying "guilty" subregions within each "guilty" region. We continue the process along each "guilty" branch of the tree until we detect the colluders at the leaf level. More specifically, at each level m, with $m=1,\ldots,M$, and with a previously identified region indexed by $\mathbf{i}=[i_1,\ldots,i_{m-1}]$, we report that the subregion indexed by $\mathbf{i}=[i_1,\ldots,i_m]$ is *colluder present* when the correlator $T_{i_1,\ldots,i_{m-1}}(i_m)$ is greater than a threshold h_m. That is, for $m=1,\ldots,(M-1)$, we define stage m in the overall detection scheme as follows.

Stage m—subregion detection at level m of the tree structure

With a previously identified region indexed by $\mathbf{i}=[i_1,\ldots,i_{m-1}]$, we need to further examine the subregions indexed by $\mathbf{i}=[i_1,\ldots,i_m]$ for $i_m=1,\ldots,L_m$. Due to the orthogonality of basis $\{\mathbf{a}_{i_1,\ldots,i_m}\}$, it suffices to consider the (normalized) correlator vector $\mathbf{T}_{i_1,\ldots,i_{m-1}}$ for identifying subregions including colluders. The i_mth component of $\mathbf{T}_{i_1,\ldots,i_{m-1}}$ is expressed by

$$T_{i_1,\ldots,i_{m-1}}(i_m)=\frac{(\mathbf{y}-\mathbf{x})^T\mathbf{a}_{i_1,\ldots,i_m}}{\sqrt{\|\mathbf{s}\|^2}}, \tag{38}$$

for $i_m=1,\ldots,L_m$. We can show that

$$p(\mathbf{T}_{i_1,\ldots,i_{m-1}}\mid K,\mathbf{S}_c,\sigma_d^2)=N(\boldsymbol{\mu}_{i_1,\ldots,i_{m-1}},\sigma_d^2\mathbf{I}_{L_m}) \tag{39}$$

with

$$\mu_{i_1,\ldots,i_{m-1}}(i_m)=\frac{k_{i_1,\ldots,i_m}\sqrt{\rho_m}}{K}\|\mathbf{s}\|, \tag{40}$$

and $k_{i_1,\ldots,i_m}=0$ indicating that no colluder is present within the subregion represented by $[i_1,\ldots,i_m]$. If many colluders belong to the sub-region represented by $[i_1,\ldots,i_m]$, we are likely to observe a large value of $T_{i_1,\ldots,i_{m-1}}(i_m)$. Therefore, the detection process in stage m is

$$\hat{\mathbf{j}}_m=\arg_{i_m=1}^{L_m}\{T_{i_1,\ldots,i_{m-1}}(i_m)\geq h_m\}, \tag{41}$$

where $\hat{\mathbf{j}}_m$ indicates the indices of subregions containing colluders within the previously identified region represented by $[i_1,\ldots,i_{m-1}]$.

Finally, we note that the individual colluders are identified at level M (the leaf level). Now with previously identified region represented by $[i_1,\ldots,i_{M-1}]$, we have, for $i_M=1,\ldots,L_M$,

$$\begin{aligned}T_{i_1,\ldots,i_{M-1}}(i_M)&=\frac{(\mathbf{y}-\mathbf{x})^T\mathbf{a}_{i_1,\ldots,i_M}}{\sqrt{\|\mathbf{s}\|^2}},\\ p(\mathbf{T}_{i_1,\ldots,i_{M-1}}\mid K,\mathbf{S}_c,\sigma_d^2)&=N(\boldsymbol{\mu}_{i_1,\ldots,i_{M-1}},\sigma_d^2\mathbf{I}_{L_m}),\end{aligned} \tag{42}$$

where

$$\mu_{i_1,\ldots,i_{M-1}}(i_M)=\begin{cases}\dfrac{\sqrt{1-\sum_{m=1}^{M-1}\rho_m}}{K}\|\mathbf{s}\|, & \text{if } k_{i_1,\ldots,i_M}>0;\\ 0, & \text{otherwise.}\end{cases} \tag{43}$$

Now the detection process in stage M is

$$\hat{\mathbf{j}}_M=\arg_{i_M=1}^{L_M}\{T_{i_1,\ldots,i_{M-1}}(i_M)\geq h_M\}, \tag{44}$$

where $\hat{\mathbf{j}}_M$ indicates the indices of colluders within the previously identified region represented by $[i_1,\ldots,i_{M-1}]$.

In our approach, at each level m, we specify a desired false positive probability α_m and choose the threshold $h_m$such that

$$P_r\{T_{i_1,\ldots,i_{m-1}}(i_m)\geq h_m\mid k_{i_1,\ldots,i_m}=0\}=Q\left(\frac{h_m}{\sigma_d}\right)=\alpha_m, \tag{45}$$

thus

$$h_m=Q^{-1}(\alpha_m)\sigma_d. \tag{46}$$

In summary, the basic idea behind this multistage detection scheme is to keep narrowing down the size of the suspicious set. An advantage of this approach is its light computational burden since, when the number of colluders K is small or the number of subregions involved in collusion is small, the total amount of correlations needed can be significantly less than the total number of users.

4.3. Parameter settings and performance analysis

In this subsection, we will address the issue of setting the parameters (e.g., how to choose the values of coefficients ρ_m's, thresholds h_m's, and the sizes L_m's) and examine the performance metrics characterized by P_{fp} and P_d. Due to the multistage nature of the proposed detection approach, calculating the overall performance P_{fp} and P_{fn} involves computing the probabilities of joint events. Furthermore, the collusion pattern will also make the analysis of P_{fp} and P_d complicated.

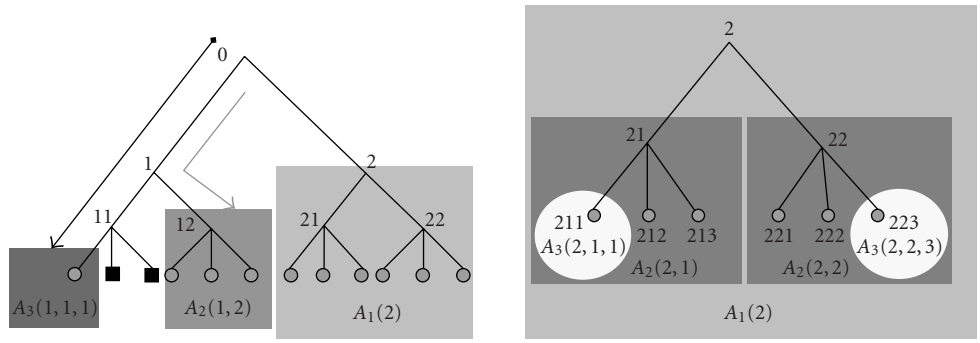


Figure 7: Demonstration of the types of false alarm events for a three-level tree structure, where at the leaf level the square-shape nodes indicate colluders and the circle-shape nodes indicate innocents. (a) The dark and light arrows represent an event in B_3 and B_2, respectively. (b) The event $A_1(2)$.

We first examine the types of false alarm events possible for our tree-structured scheme. A false alarm occurs when the detector claims colluders are present in a colluder-absent region. A colluder-absent region is characterized by $k_{i_1,\ldots,i_m} = 0$. As shown in Figure 7, where the gray rectangles represent colluder-absent regions, we can characterize false alarm events in these regions by $A_M(\cdot), A_{M-1}(\cdot), \ldots, A_1(\cdot)$:

$$\begin{aligned} A_M(i_1,\ldots,i_M) &\triangleq \{T_{i_1,\ldots,i_{M-1}}(i_M) \geq h_M \,|\, k_{i_1,\ldots,i_M} = 0\}; \\ A_m(i_1,\ldots,i_m) &\triangleq \{T_{i_1,\ldots,i_{m-1}}(i_m) \geq h_m, \\ &\qquad \cup_{i_{m+1}} A_{m+1}(i_1,\ldots,i_m,i_{m+1}) \mid k_{i_1,\ldots,i_m} = 0\}. \end{aligned} \tag{47}$$

The probability of these events is given by

$$\begin{aligned} p_M &= P_r\{A_M(i_1,\ldots,i_M)\} = \alpha_M, \\ p_m &= P_r\{A_m(i_1,\ldots,i_m)\} \\ &= \alpha_m\left[1-(1-p_{m+1})^{L_{m+1}}\right] \\ &< \alpha_m L_{m+1} p_{m+1}, \end{aligned} \tag{48}$$

for $m = (M-1),\ldots,1$. Denoting the index vectors for the estimated colluders as $\{\hat{\mathbf{i}}_c\}$, we now have

$$\begin{aligned} P_{fp} &= P_r\{\exists \hat{\mathbf{i}}_c \in \bar{\mathbf{S}}_c\} = P_r\{\cup_m B_m\}, \\ B_1 &\triangleq \{\cup_{\{i_1 | k_{i_1}=0\}} A_1(i_1)\}, \quad \text{and for } m = 2,\ldots,M, \\ B_m &\triangleq \{\cup_{\mathbf{S}_m} (T_0(i_1) \geq h_1, \ldots, T_{i_1,\ldots,i_{m-2}}(i_{m-1}) \\ &\qquad \geq h_{m-1}, A_m(i_1,\ldots,i_m))\}, \end{aligned} \tag{49}$$

where the vector set $\mathbf{S}_m = \{\{i_1,\ldots,i_m\} | \{k_{i_1} \neq 0,\ldots, k_{i_1,\ldots,i_{m-1}} \neq 0,\ k_{i_1,\ldots,i_m} = 0\}\}$. As we can see, due to the complex nature of a collusion pattern represented in the tree structure, P_{fp} is a complicated function of the collusion pattern.

During the system design process, we normally do not have knowledge of the location of the colluders. As such, we use the upper bound of P_{fp}, which does not require detailed knowledge of the collusion pattern, to guide our selection of parameter values. Let K be the total number of colluders. Based on the analysis of probability and order statistics [24, 25], as presented in Appendix B, we have

$$P_{fp} \leq \sum_{m=1}^{M} P_r\{B_m\} < L_1 p_1 + K \sum_{m=2}^{M-1} L_m p_m + K p, \tag{50}$$

where $p = 1-(1-p_M)^{L_M}$ represents the probability of a false alarm within a subregion as $[i_1,\ldots,i_{M-1}]$, where all users are innocent. As we can see, the $L_m p_m$ term in the above expression is due to the type of false alarm event A_m. Intuitively, we want the probability of an event of type A_m to decrease with a decreasing level m. In particular, we want the probability that a false alarm occurs in an innocent region connected directly to the root, $P_r\{B_1\}$ to be negligible, thus implying that α_1 is small. This is due to the fact that our tree-structured fingerprint system can be deployed in such a way that typically only a very small number of regions at the first level are involved in collusion, thus a miss-detection is rare at the first level even with a high threshold h_1. To simplify the parameter setting process, we relate the false alarm probabilities at different levels with a multiplicative factor c. That is, if at the leaf level we have the probability of a false positive represented by p, then for the $(M-1)$ level, we scale p by a factor of c and use p/c to represent the probability of the events of type B_{M-1}. We apply this scaling to upper levels in a similar way. Further, using the upper bound of p_m in (48), we can summarize the process as

$$\begin{aligned} L_{M-1}p_{M-1} &= L_{M-1}(\alpha_{M-1}p) \\ &= \frac{p}{c}, \longrightarrow \alpha_{M-1} = \frac{1}{(L_{M-1}c)}, \\ L_m p_m &< L_m(\alpha_m L_{m+1} p_{m+1}) = \frac{(L_{m+1}p_{m+1})}{c}, \\ &\longrightarrow \alpha_m = \frac{1}{(L_m c)}, \quad \text{for } m = M-2,\ldots,2. \end{aligned} \tag{51}$$

Using this choice of α_m and thus h_m in (50), we have

$$P_{fp} < Kp\left(o\left(\frac{1}{c^{M-1}}\right) + \frac{1}{c^{M-1}} + \cdots \frac{1}{c^2} + \frac{1}{c} + 1\right) < \frac{Kpc}{(c-1)}, \tag{52}$$

where $o(a)$ represents a small value compared with a, and c is a positive constant larger than 1. The detail of this derivation is provided in Appendix B. Basically, for larger K and p, or for smaller c, we will see a larger P_{fp}. Based on the chosen α_m's, we can set the threshold at level m as

$$h_m = Q^{-1}(\alpha_m)\sigma_d = Q^{-1}\left(\frac{1}{cL_m}\right)\sigma_d. \tag{53}$$

With this design scheme, we fix the thresholds at levels 1 to $(M-1)$ and only leave the threshold at the last level adjustable in our performance evaluation.

Now we proceed to study the behavior of P_d. We have

$$P_d = P_r\{\exists \hat{\mathbf{i}}_c \in \mathbf{S}_c\} = P_r\{\cup_{i_1 \in \{k_{i_1} \neq 0\}} C_1(i_1)\} \tag{54}$$

with

$$C_1(i_1) \triangleq \{T_0(i_1) \geq h_1, \cup_{i_2 \in \{k_{i_1,i_2} \neq 0\}} C_2(i_1, i_2)\}, \tag{55}$$

while for $m = 2, \ldots, (M-1)$,

$$C_m(i_1, \ldots, i_m) \triangleq \{T_{i_1,\ldots,i_{m-1}}(i_m) \geq h_m, \cup_{i_{m+1} \in \{k_{i_1,\ldots,i_{m+1}} \neq 0\}} C_{m+1}(i_1, \ldots, i_{m+1})\},$$
$$C_M(i_1, \ldots, i_M) \triangleq \{T_{i_1,\ldots,i_M} \geq h_M\}. \tag{56}$$

It is worth mentioning that, due to the independency of the basis vectors $\mathbf{a}$'s in fingerprint design, all events $C_m(\cdot)$'s at the same level m are independent of each other. Without loss of generality, given a region $\{i_1, \ldots, i_m\}$, we assume that $k_{i_1,\ldots,i_{m+1}} \neq 0$ for the first $k_{i_1,\ldots,i_{m+1}}$ indices of i_{m+1}. Therefore, we have

$$P_r\{C_m(i_1, \ldots, i_m)\} = P_r\{T_{i_1,\ldots,i_{m-1}}(i_m) \geq h_m\} \times \left[\sum_{j=1}^{k_{i_1,\ldots,i_{m+1}}} q_{i_1,\ldots,i_m}(j)\Pi_{l=1}^{j-1}(1 - q_{i_1,\ldots,i_m}(l))\right] \tag{57}$$

with $q_{i_1,\ldots,i_m}(j) = P_r\{C_{m+1}(i_1, \ldots, i_m, j)\}$. Iteratively applying this relationship, we can calculate the probability of detection P_d for a given collusion pattern. Intuitively, we can see that $P_r\{T_{i_1,\ldots,i_{m-1}}(i_m) \geq h_m\}$ plays an important role in P_d, thus the more tightly the colluders are concentrated in a subregion, the higher the P_d is. We want the probability $P_r\{T_{i_1,\ldots,i_{m-1}}(i_m) \geq h_m\}$ to be larger at lower levels, since a miss-detection in a lower level is more severe. Referring to the distribution of $T_{i_1,\ldots,i_{m-1}}(i_m)$ in (41), we note that $P_r\{T_{i_1,\ldots,i_{m-1}}(i_m) \geq h_m\}$ is characterized by the mean $\mu_{i_1,\ldots,i_{m-1}}(i_m) = k_{i_1,\ldots,i_m}\sqrt{\rho_m}\|\mathbf{s}\|/K$. Further, it is observed that

$$\max\{\mu_{i_1,\ldots,i_{m-1}}(i_m)\} \geq \frac{1}{\min\{\Pi_{j=1}^{m} L_j, K\}}\sqrt{\rho_m}\|\mathbf{s}\| = \mu_m^{\text{low}}. \tag{58}$$

From this, it is clear that $(1/K)\sqrt{\rho_m}\|\mathbf{s}\|$ is important in system design, since it characterizes the worst case of the detection performance due to higher levels (e.g., $\Pi_{j=1}^{m} L_j \geq K$). To simplify our problem, we choose $\rho_1 = \cdots = \rho_{M-1}$ and $L_2 = \cdots = L_{M-1}$. Since the final decision is made in the last level and α_M is usually low (thus h_M is large), we want to maintain enough power at the Mth level to yield reasonable detection probability. In our case, we simply choose $1 - \sum_{m=1}^{M-1} \rho_m = 0.5$, meaning half power is kept at the last level. Given the total number of users n, the WNR, and the total levels M, we choose L_1 and h_1 such that $Q((\mu_1^{\text{low}} - h_1)/\sigma_d)$ is close to 1 (e.g., 0.99) and $\alpha_1 < 1/(L_1 c)$. This strategy ensures that at least one colluder-present region will pass the detection at level 1 with very high probability. We choose L_M to maximize the number of colluders that the system can tolerate. For instance, based on the example shown in Figure 3, we can choose $L_M = 60$. Therefore, in addition to choosing L_1 and L_M as above, we set other parameters as follows by choosing:

$$\rho_1 = \cdots = \rho_{M-1} = \frac{0.5}{(M-1)}, \quad \rho_M = 0.5;$$
$$L_2 = L_3 = \cdots = L_{M-1} = \left(\frac{n}{L_1 L_M}\right)^{1/(M-2)}; \tag{59}$$
$$\alpha_m = \frac{1}{(L_m c)}, \quad \text{for } m = 2, \ldots, (M-1).$$

Now the overall performance is a function of α_M (thus h_M) and c.

We demonstrate the performance of such a fingerprinting system through examples and compare it with a fingerprinting system employing orthogonal modulation. As in the group-oriented scheme, the overall power of the colluded observation $\mathbf{y}$ is maintained as $\|\mathbf{s}\|^2$ in our simulations for a fair comparison. We consider a tree structure with four levels, where $L_1 = 8$, $L_2 = L_3 = 5$, and $L_4 = 50$, therefore it can accommodate $n = 10^4$ users. Suppose the total number of colluders $K = 40$. We first examine a scenario where the collusion pattern is balanced, that is, at each level m, all nonzero $k_{i_1,\ldots,i_m}$'s are equal. One example is illustrated in Figure 8, where we choose $\alpha_1 = 10^{-3}$ and $c = 10$. In this example, two regions at level 1 include colluders (e.g., $k_1 = k_2 = K/2$), and in turn two subregions at level 2 within each guilty region from level 1 are colluder present, then one subregion at level 3 within each guilty region of level 2 is colluder present, and finally 10 colluders are present within each guilty subregion of level 3. This example illustrates the improved collusion resistance that the tree-structured system can provide when compared to orthogonal fingerprinting.

The previous example illustrates the gain in designing fingerprints when one has precise knowledge of the collusion behavior. Sometimes, however, there might be mismatch in the assumed collusion behavior. In order to illustrate the effect of designing a group fingerprinting system for a collusion pattern that is substantially different from the true collusion pattern, we built fingerprints using the same tree structure as in the example illustrated in Figure 8. We then examined two extreme scenarios, where the collusion patterns are more random. Each collusion pattern involved 60 colluders. Random pattern 1 involves the colluders coming

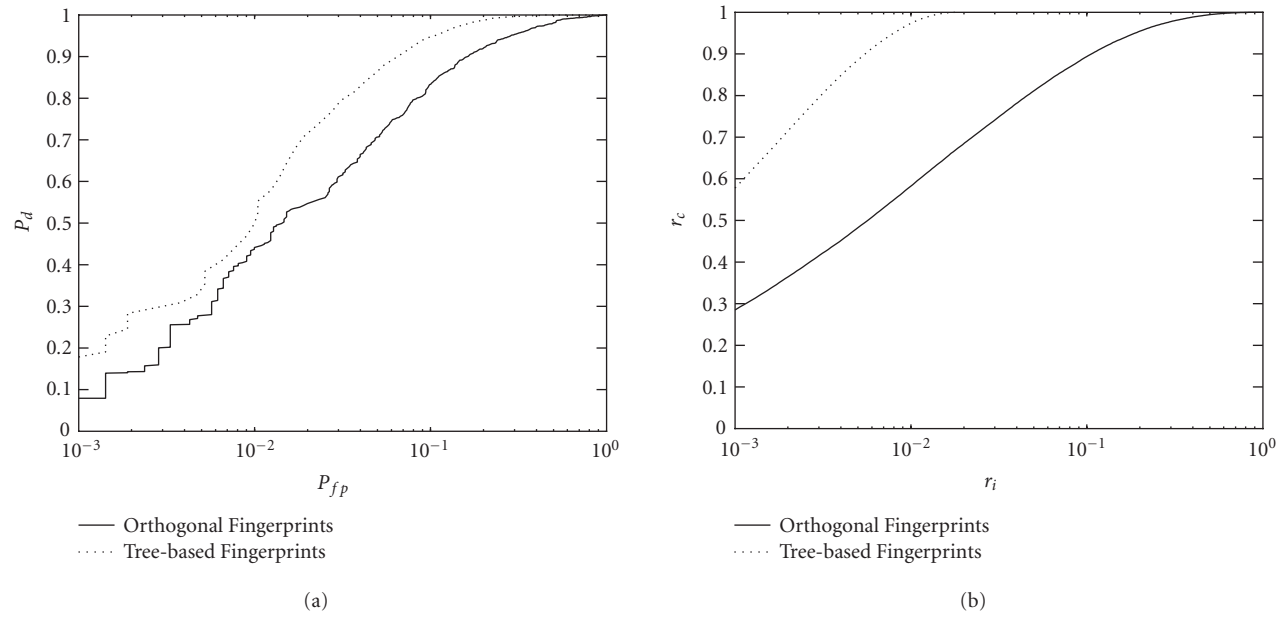


Figure 8: Performance curves of one example of the tree structure-based fingerprinting system with a symmetric collusion pattern, compared with the orthogonal scheme in [16]. Here $n = 10^4$, the number of levels $M = 4$ and $K = 4$. (a) The ROC curve P_d versus P_{fp} is plotted and (b) the curve of the fractions r_c versus r_i is shown.

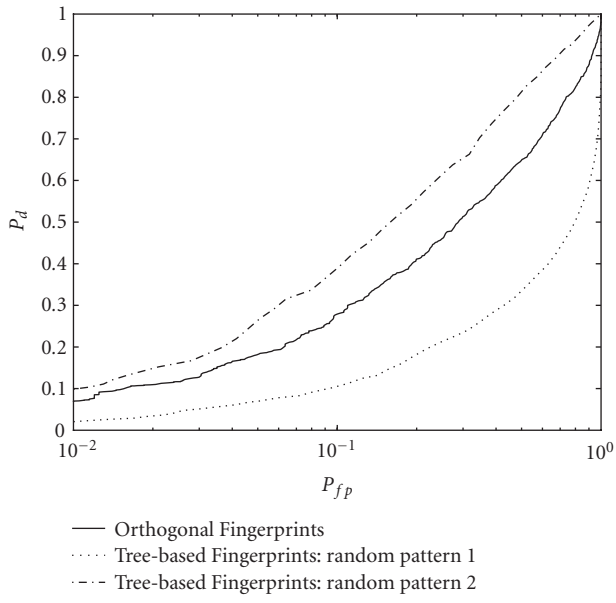


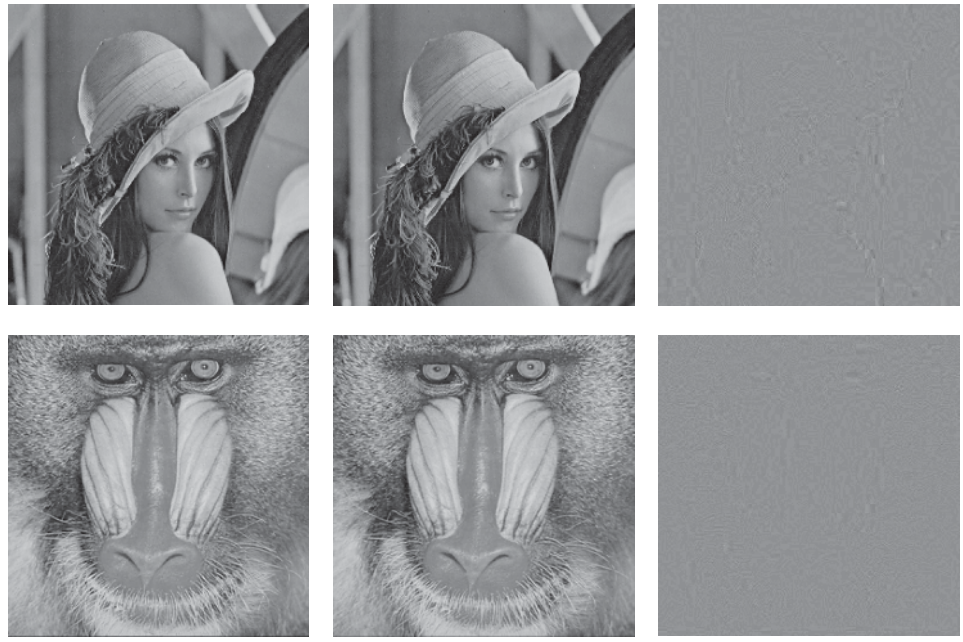
Figure 9: The ROC curve P_d versus P_{fp} of one example of the tree structure-based fingerprinting system with random collusion patterns, compared with the orthogonal scheme. Here $n = 10^4$, the number of lords $M = 4$, and $K = 60$.

together in a totally random manner, representing that all users are equally likely to collude with each other; while in random pattern 2, the colluders are randomly distributed in the first region at level 1. In Figure 9, we provide the ROC curves, P_d versus P_{fp}, for both random patterns, as well as for orthogonal fingerprints. From this figure, we have two observations: first, when the collusion pattern that the fingerprints were designed for is similar to the actual collusion pattern, as in the case of random pattern 2 at the first level, the results show improved collusion resistance. Second, when there is no similarity between the assumed collusion pattern and the true collusion pattern, as in the case of random pattern 1, orthogonal fingerprints can yield higher collusion resistance than the tree-based scheme. Therefore, it is desirable for the system designer to have good knowledge of the potential collusion pattern and design the fingerprints accordingly.

One additional advantage of the tree structure-based fingerprinting system over the orthogonal one is its computational efficiency, which is reflected by the upper bound of the expected computational burden of this approach. The upper bound is in terms of the amount of correlations required as a function of a set of parameters including the number of colluders, the threshold at each level of the tree, and the number of nodes at each level. We denote by $C(n, K)$ the number of correlations needed in our proposed detection scheme. Denoting by $E(A_m)$ the number of expected correlations needed in an event A_m and t being the number of colluder-present subregions at level $(M - 1)$, we have

$$C(n,K) < 2t \sum_{m=1}^{M} L_m < 2K \sum_{m=1}^{M} L_m. \tag{60}$$

Interested readers are referred to Appendix C for details. This bound is derived for the worst case where the number of the guilty regions at each level is set to the upper bound t. Clearly, for a small t, a situation we expect when the colluders come from the same groups, the computational cost of the tree structure-based fingerprinting system is much smaller than the n correlations needed by fingerprinting systems using orthogonal fingerprints.



(a) (b) (c)

FIGURE 10: (a) The host images, (b) colluded images with $K = 40$, and (c) difference images for Lena and Baboon under the average attack. The collusion pattern for Lena image is the same as in Figure 11, and as in Figure 12 for the Baboon image.

5. EXPERIMENTAL RESULTS ON IMAGES

We now compare the ability of our fingerprinting scheme and a system using orthogonal fingerprints for identifying colluders when deployed in actual images. In order to demonstrate the performance of orthogonal, Gaussian fingerprints, we apply an additive spread spectrum watermarking scheme similar to that in [19], where the original host image is divided into 8×8 blocks, and the watermark (fingerprint) is perceptually weighted and then embedded into the block DCT coefficients. The detection of the fingerprint is nonblind, and is performed with knowledge of the host image. To generally represent the performance, the 256×256 Lena and Baboon images were chosen as the host images since they have different characteristics. The fingerprinted images have an average PSNR of 44.6 dB for Lena, and 41.9 dB for Baboon. We compare the performance of the thresholding detector under average collusion attack. We show in Figure 10 the original host images, the colluded images, and the difference images. With $K = 40$, we obtain an average PSNR of 47.8 dB for Lena and 48.0 dB for Baboon after collusion attack and the JPEG compression.

Denoting $\mathbf{s}_j$ as the ideal Gaussian fingerprint, the ith component of the fingerprint, indexed by $\mathbf{i}_c$, is actually embedded as

$$s_{\mathbf{i}_c}(i)^t = \alpha(i) s_{\mathbf{i}_c}(i) \tag{61}$$

with $\boldsymbol{\alpha}$ being determined by the human visual model parameters in order to achieve imperceptibility. Therefore, the composite embedded fingerprint $\mathbf{y}^t$ after attacking is represented as

$$y(i)^t = \frac{1}{K}\alpha(i) \sum_{\mathbf{i}_c \in \mathbf{S}_c} s_{\mathbf{i}_c}(i) + x(i) + d(i), \tag{62}$$

where the noise d is regarded as i.i.d $N(0, \sigma_d^2)$ distributed. Due to the nonblind assumption, α_i's are known in the detector side and thus the effects of real images can be partially compensated by correlating $(\mathbf{y}^t - \mathbf{x})$ with the $\boldsymbol{\alpha}$-scaled basis or fingerprints in the test statistics $T(\cdot)$'s defined in earlier sections and adjusting the norm to be $\|\mathbf{s}^t\| = \sqrt{\sum_{i=1}^{N} \alpha(i)^2}\|\mathbf{s}\|$. For instance, the detection scheme in (41) is now defined as

$$T_{i_1,\ldots,i_{m-1}}(i_m) = \frac{(\mathbf{y}^t - \mathbf{x})^T \mathbf{a}_{i_1,\ldots,i_m}{}^t}{||\mathbf{s}^t||} \tag{63}$$

with each component $\mathbf{a}_{i_1,\ldots,i_m}(i)^t = \alpha(i)\mathbf{a}_{i_1,\ldots,i_m}(i)$.

We illustrate examples where the collusion pattern is symmetric. We consider a four-level tree structure with $L_1 = 8$, $L_2 = L_3 = 5$, and $L_4 = 50$. We present the results for the Lena image in Figure 11 based on 10^4 simulations, where $K = 40$ and we choose $\alpha_1 = 10^{-3}$ and $c = 10$. In this example, one region at level 1 is guilty, while at levels 2 and 3 we assumed that each guilty region had 2 subregions containing colluders. Finally, 10 colluders are present within each guilty sub-region at the final level, that is, level 3. Additionally, we present the results for Baboon image in Figure 12 based on 10^4 simulations, where $K = 40$, $\alpha_1 = 10^{-3}$, and $c = 10$. In this example, two regions at level 1 are guilty, while at levels 2 and 3 we assumed that each guilty

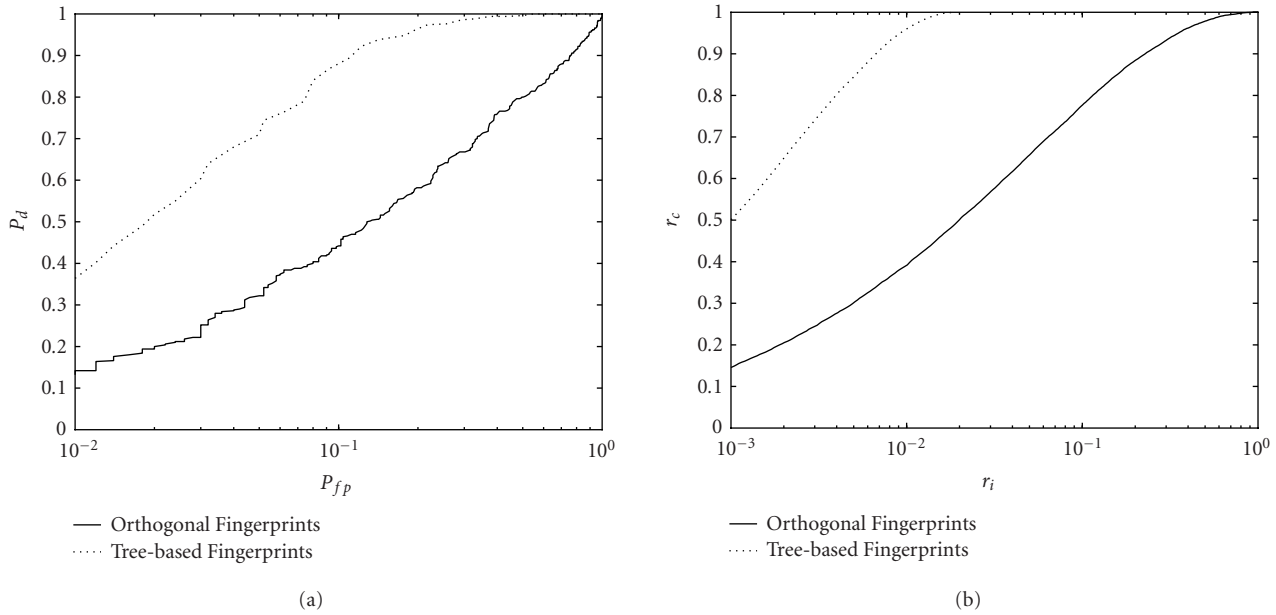


Figure 11: One example of the detection performance of the group-oriented fingerprinting system on Lena image under average attack. Here, $M = 4$, $n = 10^4$, $K = 40$, and the Lena image with equivalent $N = 13691$. (a) The curve P_d versus P_{fp}. (b) The curve r_c versus r_i.

region had 2 subregions containing colluders. Finally, 5 colluders are present within each guilty subregion at level 3. We can see that the detection performance of the proposed tree structure-based fingerprinting system is much better than that of the orthogonal system under this colluder scenario.

6. CONCLUSION

In this paper, we investigated a method for enhancing the collusion resistance performance of fingerprinting systems using orthogonal modulation. We proposed a group-oriented fingerprinting system by exploiting the fundamental property of the collusion scenario that adversaries are more likely to collude with some users than others due to geographic or social circumstances. With this underlying philosophy, we then introduced a well-controlled amount of correlations into user fingerprints in order to improve colluder identification.

We first developed a two-tier group-oriented fingerprinting system that involved the design of fingerprints and a two-stage detection scheme for identifying colluders. We evaluated the resistance performance of the proposed system under the average attack by examining different sets of performance criteria. It was demonstrated that the proposed fingerprinting scheme is superior to orthogonal fingerprinting system. In particular, as shown in one example, the proposed scheme can identify all colluders when we allow for up to 10 percent of the innocents to be wrongly accused. In stark contrast, a system using orthogonal fingerprints would require the detection system to suspect almost all users as guilty.

Our work was further extended to a more flexible tree structure-based fingerprinting system in order to represent the natural hierarchical relationships between users due to social and geographic circumstances. We proposed an efficient and simple scheme for fingerprint design, and proposed a multistage colluder identification scheme by exploiting the hierarchical nature of the group-oriented system where the basic idea is to successively narrow down the size of the suspicious set. Performance criteria were analyzed to guide the parameter settings during the design process. We demonstrated performance improvement of the proposed scheme over the orthogonal scheme via examples. Furthermore, we derived an upper bound on the expected computational burden of the proposed approach and showed that one additional advantage of the tree structure-based fingerprinting system is its computational efficiency. We also evaluated the performance on real images and noted that the experimental results match the analysis. Overall, by exploiting knowledge of the dynamics between groups of colluders, our proposed scheme illustrates a promising mechanism for enhancing the collusion resistance performance of a multimedia fingerprinting system.

APPENDICES

A. DERIVATION OF (11) AND (13)

Recall the distribution and the correlation coefficients

$$p(\mathbf{T}_i \mid K, S_{ci}, \sigma_d^2) = N\left(\frac{\|\mathbf{u}\|}{K}\mathbf{C}\boldsymbol{\Phi}_i, \sigma_d^2\mathbf{I}_M\right),$$
$$\mathbf{c}_j^T\mathbf{c}_l = \begin{cases} 1, & \text{if } j = l, \\ \rho, & \text{if } j \neq l. \end{cases} \tag{A.1}$$

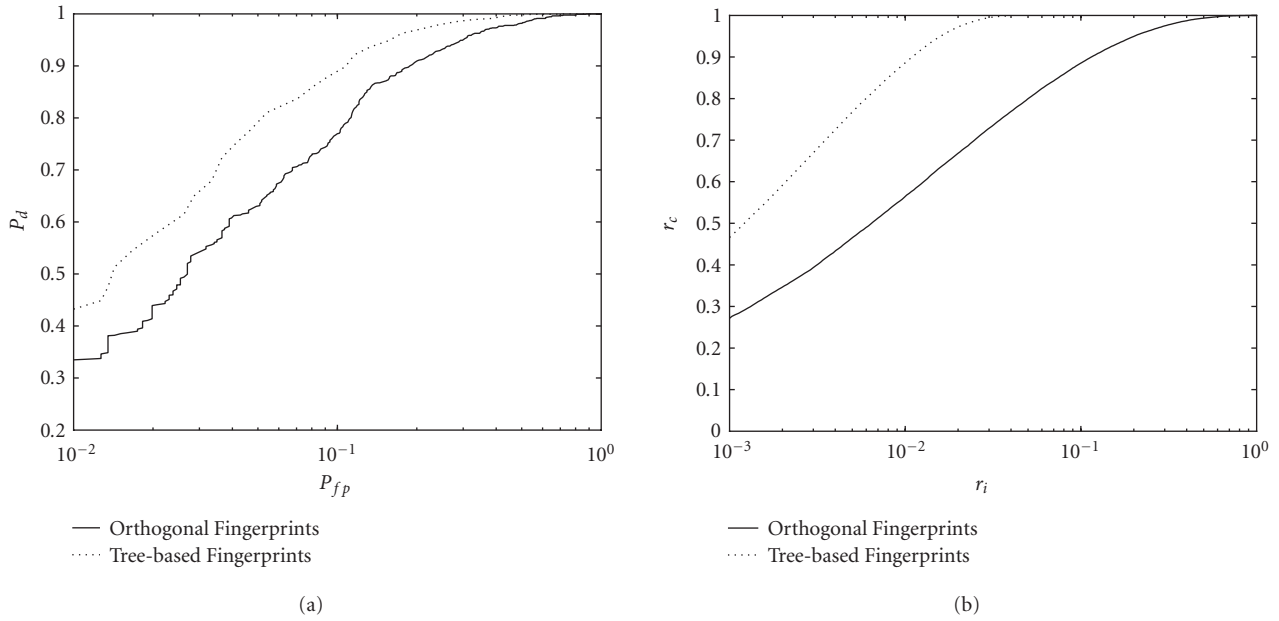


Figure 12: One example of the detection performance of the group-oriented fingerprinting system on Baboon image under average attack. Here, $M = 4$, $n = 10^4$, $K = 40$, and the Baboon image with equivalent $N = 19497$. (a) The curve P_d versus P_{fp}. (b) The curve r_c versus r_i.

Now assume the parameters K and k_i are known, we can estimate the subset S_{ci} via

$$\begin{aligned}
\hat{S}_{ci} &= \arg\max_{|S_{ci}|=k_i} \{p(\mathbf{T}_i \mid K, S_{ci}, \sigma_d^2)\} \\
&= \arg\min_{|S_{ci}|=k_i} \left\| \mathbf{T}_i - \frac{\|\mathbf{u}\|}{K} \mathbf{C}\Phi_i \right\|^2 \\
&= \arg\min_{|S_{ci}|=k_i} \left\{ \mathbf{T}_i^T \mathbf{T}_i - \frac{2\|\mathbf{u}\|}{K} \sum_{j\in S_{ci}} \mathbf{T}_i^T \mathbf{c}_j \right. \\
&\qquad \left. + \frac{\|\mathbf{u}\|^2}{K^2} \left(\sum_{j\in S_{ci}} \mathbf{c}_j \right)^T \left(\sum_{j\in S_{ci}} \mathbf{c}_j \right) \right\} \qquad \text{(A.2)} \\
&= \arg\min_{|S_{ci}|=k_i} \left\{ \mathbf{T}_i^T \mathbf{T}_i - \frac{2\|\mathbf{u}\|}{K} \sum_{j\in S_{ci}} \mathbf{T}_i^T \mathbf{c}_j \right. \\
&\qquad \left. + \frac{\|\mathbf{u}\|^2}{K^2} [k_i + (k_i^2 - k_i)\rho] \right\} \\
&= \arg\max_{|S_{ci}|=k_i} \left\{ \frac{2\|\mathbf{u}\|}{K} \sum_{j\in S_{ci}} \mathbf{T}_i^T \mathbf{c}_j \right\} \\
&= \text{the indices of } k_i \text{ largest } T_{si}(j)\text{'s},
\end{aligned}$$

where the vector $\mathbf{T}_{si}$ is defined as

$$\mathbf{T}_{si} = \mathbf{C}_i^T \mathbf{T}_i = \mathbf{C}^T \left[\frac{\mathbf{U}_i^T (\mathbf{y} - \mathbf{x})}{\|\mathbf{u}\|} \right] = \frac{\mathbf{S}_i^T (\mathbf{y} - \mathbf{x})}{\|\mathbf{s}\|} \qquad \text{(A.3)}$$

since $\|\mathbf{s}\| = \|\mathbf{u}\|$. We can see that $\mathbf{T}_{si}$ are the correlation statistics involving the colluded observation $\mathbf{y}$, the host signal $\mathbf{x}$, and the fingerprints $\mathbf{s}_{ij}$'s. Since $\mathbf{T}_{si} = \mathbf{C}^T \mathbf{T}_i$, $\mathbf{T}_{si}$ conditioned on K and S_{ci} is also Gaussian distributed with the mean vector and the covariance matrix decided as

$$\boldsymbol{\mu}_i = \mathbf{C}^T E\{\mathbf{T}_i \mid K, S_{ci}, \sigma_d^2\} = \frac{\|\mathbf{u}\|}{K} \mathbf{R}\Phi_i, \qquad \text{(A.4)}$$

thus

$$\mu_i(j) = \begin{cases} \dfrac{1 + (k_i - 1)\rho}{K} \|\mathbf{s}\|, & \text{if } j \in S_{ci}, \\ \dfrac{k_i \rho}{K} \|\mathbf{s}\|, & \text{otherwise}, \end{cases} \qquad \text{(A.5)}$$

$$R = \mathbf{C}^T \operatorname{Cov}\{\mathbf{T}_i \mid K, S_{ci}, \sigma_d^2\} \mathbf{C} = \sigma_d^2 \mathbf{R},$$

according to the properties of the vector-valued Gaussian distribution [26].

B. DERIVATION OF (52)

Based on the expression of P_{fp} in (49), we have $P_{fp} \le \sum_{m=1}^{M} P_r\{B_m\}$. Recall the definition of B_m's and that $\sum_{i_1=1}^{L_1} \cdots \sum_{i_m=1}^{L_m} k_{i_1,\ldots,i_m} = K$. We note that the size $|\mathbf{S}_1| = |\{i_1 \mid k_{i_1} = 0\}| \le L_1$, the size of the colluder-present regions satisfying $\{k_{i_1} \ne 0, \ldots, k_{i_1,\ldots,i_{m-1}} \ne 0\}$ is smaller than K, and therefore that the size of $\mathbf{S}_m$ satisfies $|\mathbf{S}_m| \le KL_m$ for $m = 2, \ldots, M$. Therefore, by taking advantage of the independency of the basis vectors $\mathbf{a}$'s, we have

$$P_r\{B_1\} \le 1 - (1 - p_1)^{L_1} < L_1 p_1, \qquad \text{(B.1)}$$

and for $m = 2, \ldots, M$

$$\begin{aligned} P_r\{B_m\} &\le KP_r\{T_0(i_1) \ge h_1, \ldots, T_{i_1,\ldots,i_{m-2}}(i_{m-1}) \\ &\qquad \ge h_{m-1}, \cup_{i_m} A_m(i_1, \ldots, i_m)\}\}, \\ &= K\Pi_{j=1}^{m-1} P_r\{T_{i_1,\ldots,i_{j-1}}(i_j) \ge h_{m-1}\} \\ &\quad \times P_r\{\cup_{i_m} A_m(i_1, \ldots, i_m)\}\} \\ &\le KP_r\{\cup_{i_m} A_m(i_1, \ldots, i_m)\}\} \\ &\le K\left[1 - (1 - p_m)^{L_m}\right] < KL_m p_m. \end{aligned} \tag{B.2}$$

By defining $p = [1 - (1 - p_M)^{L_M}]$ in the above, we have $P_r\{B_M\} \le Kp$. Putting all these inequalities together, we have

$$P_{fp} \le \sum_{m=1}^{M} P_r\{B_m\} \le L_1 p_1 + K \sum_{m=2}^{M-1} L_m p_m + Kp. \tag{B.3}$$

By choosing $\alpha_m = 1/(L_m c)$ and using that $p_m < \alpha_m L_{m+1} p_{m+1}$ for $m = 1, \ldots, (M-1)$, and choosing α_1 such that $P_r\{B_1\}$ is negligible in comparison with other terms $P_r\{B_m\}$'s, we now have $P_{fp} < Kp(1 + 1/c + 1/c^2 + \cdots + 1/c^{M-1} + o(1/c^{M-1})) < 2Kp$. Therefore, (52) is obtained.

C. DERIVATION OF (60)

We denote by $C(n, K)$ the number of correlations needed in our proposed detection scheme. Denoting by $E(A_m)$ the number of expected correlations needed in an event A_m, t being the number of colluder-present subregions at level $(M-1)$, and C (detection) and C (false alarm) being the number of expected correlations needed in correct detections and false alarms, respectively, we have

$$C(n, K) = C \text{ (detection)} + C \text{ (false alarm)}. \tag{C.1}$$

Suppose all the detections for colluder-present subregions are truthful, meaning no miss-detection occurs at any stage, then

$$C \text{ (detection)} \le L_1 + tL_2 + \cdots + tL_m < t \sum_{m=1}^{M} L_m. \tag{C.2}$$

Recalling that the false alarms can be categorized into event types A_m's and that the number of each type of event A_m is less that tL_m, we have

$$C \text{ (false alarm)} \le L_1 E(A_1) + t \sum_{m=2}^{M-1} L_m E(A_m) \tag{C.3}$$

with

$$\begin{aligned} E(A_{M-1}) &= \alpha_{M-1} L_M, \\ E(A_m) &= \alpha_m L_{m+1} E(A_{m+1}) = \cdots = \alpha_m (\Pi_{j=m+1}^{M-1} L_j \alpha_j) L_M \\ &= \alpha_m \frac{1}{c^{M-(m+1)}} L_M, \quad \text{for } m = 1, \ldots, (M-2), \end{aligned} \tag{C.4}$$

by referring to $\alpha_m = 1/(L_m c)$. Therefore,

$$\begin{aligned} C \text{ (false alarm)} &< t \sum_{m=1}^{M-1} L_m \alpha_m \frac{1}{c^{M-(m+1)}} L_M \\ &= t \sum_{m=1}^{M-1} \frac{1}{c^{M-m}} L_M \\ &< \min\left\{M, \frac{1}{(c-1)}\right\} K L_M \\ &< \min\left\{M, \frac{1}{(c-1)}\right\} t \sum_{m=1}^{M} L_m. \end{aligned} \tag{C.5}$$

Putting C (detection) and C (false alarm) together, and assuming $c \ge 2$ usually, we have

$$C(n, K) < \left(1 + \min\left\{M, \frac{1}{(c-1)}\right\}\right) t \sum_{m=1}^{M} L_m < 2t \sum_{m=1}^{M} L_m. \tag{C.6}$$

Therefore, (60) is obtained. In addition, the above bound is loose, since it is derived for the worst case where the number of the guilty regions at each level is set as the upper bound t.

ACKNOWLEDGMENT

This work was supported in part by the Air Force Research Laboratory under DDET Grant no. F30602-03-2-0045 and the National Science Foundation under CAREER Award no. CCR-0133704.

REFERENCES

[1] I. J. Cox, J. Bloom, and M. Miller, *Digital Watermarking: Principles & Practices*, Morgan Kaufmann Publishers, San Francisco, Calif, USA, 2001.

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

[3] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual watermarks for digital images and video," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1108–1126, 1999.

[4] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—a survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999.

[5] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," *Proceedings of the IEEE*, vol. 86, no. 6, pp. 1064–1087, 1998.

[6] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1079–1107, 1999.

[7] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 1897–1905, 1998.

[8] H.-J. Guth and B. Pfitzmann, "Error—and collusion-secure fingerprinting for digital data," in *Proc. 3rd International Workshop on Information Hiding*, pp. 134–145, Springer-Verlag, Dresden, Germany, September–October 1999.

[9] J. Domingo-Ferrer and J. Herrera-Joancomart, "Simple collusion-secure fingerprinting schemes for images," in

Proc. IEEE International Conference on Information Technology: Coding and Computing (ITCC '00), pp. 128–132, Las Vegas, Nev, USA, March 2000.

[10] W. Trappe, M. Wu, and K. J. R. Liu, "Collusion-resistant fingerprinting for multimedia," in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing (ICASSP '02)*, vol. 4, pp. 3309–3312, Orlando, Fla, USA, May 2002.

[11] W. Trappe, M. Wu, Z. J. Wang, and K. J. R. Liu, "Anti-collusion fingerprinting for multimedia," *IEEE Trans. on Signal Processing*, vol. 51, no. 4, pp. 1069–1087, 2003, Special issue on Signal Processing for Data Hiding in Digital Media & Secure Content Delivery.

[12] F. Ergun, J. Kilian, and R. Kumar, "A note on the limits of collusion-resistant watermarks," in *Advances in Cryptology (EUROCRYPT '99)*, pp. 140–149, Prague, Czech Republic, May 1999.

[13] J. Kilian, T. Leighton, L. Matheson, T. Shamoon, R. Tarjan, and F. Zane, "Resistance of digital watermarks to collusive attacks," in *Proc. IEEE International Symposium on Information Theory (ISIT '98)*, p. 271, Cambridge, Mass, USA, August 1998.

[14] J. Su, J. Eggers, and B. Girod, "Capacity of digital watermarks subjected to an optimal collusion attack," in *Proc. European Signal Processing Conference (EUSIPCO '00)*, vol. 4, Tampere, Finland, September 2000.

[15] H. Stone, "Analysis of attacks on image watermarks with randomized coefficients," Tech. Rep., NEC Research Institute, Princeton, NJ, USA, 1996.

[16] Z. J. Wang, M. Wu, H. Zhao, W. Trappe, and K. R. Liu, "Collusion resistance of multimedia fingerprinting using orthogonal modulation," in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing (ICASSP '03)*, Hong Kong, April 2003.

[17] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information hiding," *IEEE Transactions on Information Theory*, vol. 49, no. 3, pp. 563–593, 2003.

[18] B. Chen and G. W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423–1443, 2001.

[19] C. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 525–539, 1998.

[20] M. Wu and B. Liu, "Modulation and multiplexing techniques for multimedia data hiding," in *Proc. SPIE Information Technologies and Communications (ITcom '01)*, vol. 4518 of *Proceedings of SPIE*, pp. 228–238, Denver, Colo, USA, August 2001.

[21] M. Wu and B. Liu, "Data hiding in image and video. Part-I. Fundamental issues and solutions," *IEEE Trans. Image Processing*, vol. 12, no. 6, pp. 685–695, 2003.

[22] A. Herrigel, J. J. K. O'Ruanaidh, H. Petersen, S. Pereira, and T. Pun, "Secure copyright protection techniques for digital images," in *Proc. 2nd International Workshop on Information Hiding*, vol. 1525 of *Lecture Notes in Computer Science*, pp. 169–190, Springer-Verlag, Portland, Ore, USA, April 1998.

[23] J. Proakis, *Digital Communications*, McGraw-Hill, New York, NY, USA, 4th edition, 2000.

[24] N. Balakrishnan and C. R. Rao, Eds., *Order Statistics: Theory and Methods*, Elsevier Science B. V., Amsterdam, Netherlands, 1998.

[25] H. Stark and J. Woods, Eds., *Probability and Random Processes with Applications to Signal Processing*, Prentice Hall, Englewood Cliffs, NJ, USA, 3rd edition, 2002.

[26] S. Haykin, *Adaptive Filter Theory*, Prentice Hall, Englewood Cliffs, NJ, USA, 1996.

Z. Jane Wang received the B.S. degree from Tsinghua University, China, in 1996, with the highest honor, and the M.S. and Ph.D. degrees from the University of Connecticut in 2000 and 2002, respectively, all in electrical engineering. While at the University of Connecticut, Dr. Wang received the Outstanding Engineering Doctoral Student Award. She is currently an assistant professor at the Electrical and Computer Engineering Department at the University of British Columbia. Previously, she held the position of a Research Associate at the Department of Electrical and Computer Engineering, and the Institute for Systems Research at the University of Maryland, College Park. Her research interests are in the broad area of statistical signal processing, information security, genomic signal processing and statistics, and wireless communications.

Min Wu received the B.E. degree in electrical engineering and the B.A. degree in economics from Tsinghua University, Beijing, China, in 1996 (both with the highest honors), and the M.A. degree and Ph.D. degree in electrical engineering from Princeton University in 1998 and 2001, respectively. She was with NEC Research Institute and Signafy Inc. in 1998, and with Panasonic Information and Networking Laboratories in 1999. Since 2001, she has been an Assistant Professor of the Department of Electrical and Computer Engineering, at the Institute of Advanced Computer Studies, and the Institute of Systems Research at the University of Maryland, College Park. Dr. Wu's research interests include information security, multimedia signal processing, and multimedia communications. She received a CAREER award from the U.S. National Science Foundation in 2002 and a George Corcoran Faculty Award from University of Maryland in 2003. She coauthored a book, *Multimedia Data Hiding* (Springer-Verlag, 2003), and holds four U.S. patents on multimedia security. She is a member of the IEEE Technical Committee on Multimedia Signal Processing, Publicity Chair of 2003 IEEE International Conference on Multimedia and Expo, and a guest editor of the Special Issue on Media Security and Rights Management for the EURASIP Journal on Applied Signal Processing.

Wade Trappe received his B.A. degree in mathematics from The University of Texas at Austin in 1994 and the Ph.D. in applied mathematics and scientific computing from the University of Maryland in 2002. He is currently an assistant professor at the Wireless Information Network Laboratory (WINLAB) and the Electrical and Computer Engineering Department at Rutgers University. His research interests include multimedia security, cryptography, wireless network security, and computer networking. While at the University of Maryland, Dr. Trappe received the George Harhalakis Outstanding Systems Engineering Graduate Student Award. Dr. Trappe is a coauthor of the textbook *Introduction to Cryptography with Coding Theory*, (Prentice Hall, 2001). He is a member of the IEEE Signal Processing, Communication, and Computer societies.

K. J. Ray Liu received the B.S. degree from the National Taiwan University in 1983, and the Ph.D. degree from UCLA in 1990, both in electrical engineering. He is a Professor of Electrical and Computer Engineering Department and Institute for Systems Research of University of Maryland, College Park. His research contributions encompass broad aspects of signal processing algorithms and architectures; multimedia communications and signal processing; wireless communications and networking; information security; and bioinformatics, in which he has published over 300 refereed papers. Dr. Liu is the recipient of numerous honors and awards including IEEE Signal Processing Society 2004 Distinguished Lecturer, the 1994 National Science Foundation Young Investigator Award, the IEEE Signal Processing Society's 1993 Senior Award (Best Paper Award), IEEE 50th Vehicular Technology Conference Best Paper Award, Amsterdam, 1999 and EURASIP 2004 Meritorious Service Award. He also received the George Corcoran Award in 1994 for outstanding contributions to electrical engineering education and the Outstanding Systems Engineering Faculty Award in 1996 in recognition of outstanding contributions in interdisciplinary research, both from the University of Maryland. Dr. Liu is a Fellow of the IEEE. Dr. Liu is the Editor-in-Chief of IEEE Signal Processing Magazine and was the founding Editor-in-Chief of EURASIP Journal on Applied Signal Processing. Dr. Liu is a Board of Governor and has served as Chairman of Multimedia Signal Processing Technical Committee of IEEE Signal Processing Society.