ANTI-COLLUSION OF GROUP-ORIENTED FINGERPRINTING

Z. Jane Wang, Min Wu, Wade Trappe**, and K. J. Ray Liu*

* ECE Department and ISR, University of Maryland, College Park
$**$ WINLAB and ECE Department, Rutgers University
Email: wangzhen, minwu, kjrliu@eng.umd.edu; wxt@eng.umd.edu

ABSTRACT

Digital fingerprinting of multimedia data involves embedding information in the content, 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 fingerprints 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, since an adversary is more likely to collude with some users than other users, we propose a group-based fingerprinting scheme where users likely to collude with each other are assigned correlated fingerprints. We evaluate the performance of our group-based fingerprints by studying the collusion resistance of a fingerprinting system employing Gaussian distributed fingerprints. We compare the results to those of fingerprinting systems employing orthogonal modulation.

1. INTRODUCTION AND PROBLEM DESCRIPTION

With the rapid deployment of multimedia technologies and the substantial growth in the use of the Internet, digital protection of multimedia data has become increasingly critical. Digital fingerprinting is an effort to offer such protection by providing a means for authorized parties to identify fingerprints embedded in the multimedia content. There is, however, a class of cost-effective and powerful attacks, called *collusion* attacks, whereby a coalition of users combine their different marked copies of the same media content in an attempt to attenuate/remove the trace of any original fingerprint. The fingerprint must therefore survive both standard distortions and collusion attacks. Several methods have been proposed in the literature to embed and hide fingerprints (watermarks) in different media [2, 3]. The spread spectrum watermarking method, where the watermarks have a componentwise Gaussian distribution and are statistically independent, was argued to be highly resistant to collusion attacks [3, 5].

The research on the collusion-resistant fingerprinting systems include designing collusion-resistant fingerprint codes [1, 8], and examining the resistance performance of specific watermarking schemes under different attacks. We are aware of only a few works on the latter [4, 5, 6, 7]. Proposing a simple linear collusion attack that consists of adding noise to the average of K independent copies, the authors concluded in [5] 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 non-negligible probability, when Gaussian watermarks are considered. It was further shown to be optimal: no other watermarking scheme can offer better collusion resistance[5]. These results are also supported by [4]. Stone suggested that the most powerful attack may succeed to defeat uniformly distributed watermarks if as few as one to two dozen independent copies are available [7]. In our previous work, we analyzed the collusion resistance of an orthogonal fingerprinting system under different attacks when employing different performance criteria, and derived lower and upper bounds for the maximum number of colluders needed to thwart the system[9].

Regardless of 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 [4, 5, 9]. Therefore, an alternative fingerprinting scheme is needed that will exploit a different aspect of the collusion problem in order to achieve improved collusion resistance. To accomplish this, we propose to exploit the fact that adversaries are more likely to collude with some users than others. We propose an alternative fingerprinting scheme which still employs Gaussian watermarks but assigns correlated fingerprints to members of a group of potential colluders while the fingerprints assigned to different groups are independent of each other. Throughout this paper, we consider additive embedding, a general watermarking scheme, where a watermark signal is added to a host signal, and will focus entirely on the averaging form of collusion attack.

2. THE PROPOSED FINGERPRINTING SCHEME

Fingerprinting systems using orthogonal modulation do not consider the following issues:

1. Orthogonal fingerprinting schemes are designed for the equal possibility of collusion among all users. However, some groups of users are more likely to come together and carry out collusion (i.e. users from the same region, or users sharing the same cultural background).
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 [9] 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.
3. The performance can be improved by applying appropriate detection strategies. The challenge is to take advantages of the previous points in designing the detection process.

By considering these issues, we improve on the orthogonal fingerprinting system, and provide a means to enhance the collusion

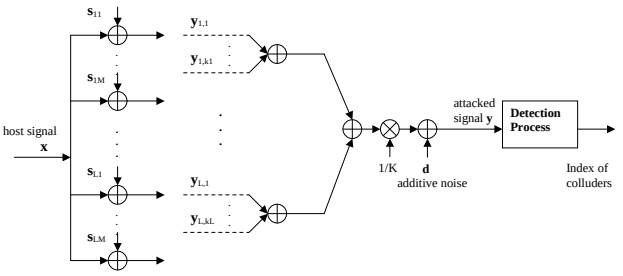


Fig. 1. Model for collusion by averaging.

resistance performance. To accomplish this, we design a fingerprinting system by employing grouping and code modulation.

Grouping: the overall fingerprinting system is implemented by designing L sub-systems. For simplicity, we assume that each subsystem 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 one region, and the collusion pattern of users. We also assume that fingerprints assigned to different groups are independent of each other. Two main advantages are provided by independency among groups. First, the detection process is simple to carry out, and secondly, when collusion occurs, the independency among groups helps to limit the innocents under suspicion within one group, since the possibility to wrongly accuse 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 M orthogonal basis signals $\mathbf{U} = [\mathbf{u}_{i1}, \mathbf{u}_{i2}, ..., \mathbf{u}_{iM}]$, each is with the Euclidean norm $\| \mathbf{u} \|$. These sets of orthogonal basis for different groups are also independent. In code modulation, information is encoded into $\mathbf{s}_{ij}$, the j^{th} fingerprint in group i, via

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

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

$$\mathbf{R}_s = \| \mathbf{u} \|^2 \mathbf{R}, \text{ with } \mathbf{R} = \mathbf{C}^T \mathbf{C}.$$

As we can see, a key point in designing the set of fingerprints is to select the 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 would like to have the fingerprints in one group equally correlated. Therefore, we choose a matrix $\mathbf{R}$ such that all its diagonal elements are set as 1 and all its off-diagonal elements are set as ρ. It is clear that the correlation matrix is fully characterized by the coefficient ρ.

Based on this proposed fingerprinting scheme, we need to address such issues as the size of groups and the coefficient ρ. The parameters M and ρ shall be chosen to yield a good system performance.

3. DETECTION SCHEME

In this section we discuss the problem of detecting the colluders when the above scheme is considered. As in Fig. 1, the system accommodates n users, consisting of L groups with M users within each group. When a collusion occurs, suppose that totally K colluders are involved in forming a colluded content copy $\mathbf{y}$, and the number of colluders within group i is k_i satisfying $\sum_{i=}^{L} k_i = K$. The observed content $\mathbf{y}$ after the average collusion is

$$\mathbf{y} = \frac{1}{K} \sum_{i=1}^{L} \sum_{j \in S_{ci}} \mathbf{y}_{ij} + \mathbf{d} = \frac{1}{K} \sum_{i=1}^{L} \sum_{j \in S_{ci}} \mathbf{s}_{ij} + \mathbf{x} + \mathbf{d} \tag{2}$$

where $S_{ci} \subseteq [1, ..., M]$, indicates a subset of size $|S_{ci}| = k_i$, and $\mathbf{s}_{ij}$'s are Gaussian distributed. We also assume 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 non-blind 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 including 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 including colluders. The $i-th$ component of $\mathbf{T}_G$ is expressed by

$$T_G(i) = \frac{(\mathbf{y} - \mathbf{x})^T (\mathbf{s}_{i1} + \mathbf{s}_{i2} + ... + \mathbf{s}_{iM})}{\sqrt{\|\mathbf{s}\|^2 [M + (M^2 - M)\rho]}} \tag{3}$$

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

$$p(T_G(i)|K, k_i, \sigma_d^2) = \begin{cases} N(0, \sigma_d^2), & \text{if } k_i = 0 \\ N(\frac{k_i \|\mathbf{s}\| \sqrt{1+(M-1)\rho}}{K\sqrt{M}}, \sigma_d^2), & \text{otherwise.} \end{cases} \tag{4}$$

where $T_G(i)$ is independent of each other. If no colluder is present in group i, $T_G(i)$ will only consist of small contributions. If more colluders belong to group i, we are likely to get a larger value of $T_G(i)$. We compare $T_G(i)$ to a threshold h_G, and report that the $i-th$ group is *colluder-present* if $T_G(i)$ exceeds h_G. That is,

$$\hat{\mathbf{i}} = \arg \max_{i=1}^{L} \{T_G(i) \geq h_G\} \tag{5}$$

where the set $\hat{\mathbf{i}}$ indicates the indices of groups including colluders. As indicated in the distribution (4), the threshold h_G here is determined by the pdf. Since normally the number of groups involving in the collusion is small, we can correctly classify groups with high probability under the non-blind 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 $[\mathbf{u}_{i1}, \mathbf{u}_{i2}, ..., \mathbf{u}_{iM}]$, it is sufficient to consider the correlators $\mathbf{T}_i$, with $T_i(j) = \frac{(\mathbf{y}-\mathbf{x})^T \mathbf{u}_{ij}}{\sqrt{\|\mathbf{u}\|^2}}$ for $j = 1, ..., M$. Suppose the parameters K and k_i's are assumed known, we can estimate the subset S_{ci} via

$$\begin{aligned} \hat{S}_{ci} &= \arg \max_{|S_{ci}|=k_i} p(\mathbf{T}_i | K, S_{ci}, \sigma_d^2) \\ &= \text{the indices of the } k_i \text{ largest } T_{si}(j)\text{'s} \end{aligned} \tag{6}$$

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

and we can show that $\mathbf{T}_{si}$ has the distribution

$$\begin{aligned} p(\mathbf{T}_{si}|K, S_{ci}, \sigma_d^2) &= N(\mu_i, \sigma_d^2 \mathbf{R}), \qquad (7) \\ \text{where } \mu_i(j) &= \begin{cases} \frac{1+(k_i-1)\rho}{K} \| \mathbf{s} \|, & \text{if } j \in S_{ci} \\ \frac{k_i \rho}{K} \|\mathbf{s}\|, & \text{otherwise .} \end{cases} \end{aligned}$$

However, applying (6) to locate colluders is not preferred due to two concerns. One is that the knowledge of K and k_i is usually not available in practice, and needs to be estimated. For the remainder of this paper, however, we assume that the detector knows K and k_i. In addition, the above approach aims to minimize the joint estimation error of all colluders, and it lacks of the capability in adjusting parameters to satisfy specific system requirements. Regardless of these concerns, the observation in (6) suggests the use of $\mathbf{T}_{si}$ to detect colluders within each group. Therefore, we employ a simple detection approach by comparing $T_{si}(j)$ to a threshold h_i and indicating a colluder-presence whenever $T_{si}(j)$ is greater than h_i. That is,

$$\hat{\mathbf{j}}_i = \arg \max_{j=1}^{M} \{\mathbf{T}_{si}(j) \geq h_i\} \qquad (8)$$

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

In our approach, we choose the thresholds such that

$$\begin{aligned} Pr\{T_G(i) \geq h_G | k_i = 0\} &= Q(h_G/\sigma_d) = \alpha_1, \qquad (9) \\ Pr\{T_{si}(j) \geq h_i | k_i, j \notin S_{ci}\} &= Q\left(\frac{h_i - k_i \rho \|s\|/K}{\sigma_d}\right) = \alpha_2, \end{aligned}$$

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

4. PERFORMANCE ANALYSIS

The purpose of this section is to show the performance of the above system under one of the most popular criteria: the probability of a false negative P_{fn} (failing to identify any of the colluders) compared to the probability of a false positive P_{fp} (falsely indicating that an innocent user is a colluder). For convenience, we shall use the probability of detection $P_d = 1 - P_{fn}$ in our analysis. The goal of this criteria is to catch at least one colluder with high confidence. We note that other performance criteria might arise under different situations, such as described in [9], and do not present results for these criteria due to space considerations. To compare with the orthogonal scheme [9], we assume the overall MSE (mean-square-error) introduced to the host signal is constant. More specifically,

$$E\{\| \mathbf{y}-\mathbf{x} \|^2\} = \left(\frac{1-\rho}{K} + \frac{\rho \sum_{i=1}^{L} k_i^2}{K^2}\right) \| \mathbf{s} \|^2 + N\sigma_d^2 \triangleq \xi_0 = \| \mathbf{s} \|^2,$$

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

One factor of great concern here is the coefficient ρ. When the total number of users is small, for instance $n \leq 100$, all the users will belong to one or two groups, a situation where Stage 1 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 mean difference $(1-\rho)\|\mathbf{s}\|/K$ as referring to (7), therefore a negative ρ is preferred. Since the matrix $\mathbf{R}$ should be positive definite, $1 + (M-1)\rho > 0$ is required. On the other hand, suppose that the fingerprinting system is designed to accommodate a large number of users, then Stage 1 is of critical importance and thus a positive coefficient ρ should be employed to yield high accuracy in group detection. In this case, we design fingerprints $\{\mathbf{s}_{ij}\}$'s in a simple way,

$$\mathbf{s}_{ij} = \sqrt{1-\rho}\mathbf{e}_{ij} + \sqrt{\rho}\mathbf{a}_i, \qquad (10)$$

where $\{\mathbf{e}_{i1}, ..., \mathbf{e}_{iM}, \mathbf{a}_i\}$ are orthogonal basis vectors of group i with equal energy. The bases of different groups are independent. Now we have $T_{si}(j) = T_{ei}(j) + T_a(i)$, with

$$\begin{aligned} &T_{ei}(j) = \frac{\sqrt{1-\rho}(\mathbf{y}-\mathbf{x})^T \mathbf{e}_{ij}}{\sqrt{\| \mathbf{s} \|^2}}, \quad T_a(i) = \frac{\sqrt{\rho}(\mathbf{y}-\mathbf{x})^T \mathbf{a}_i}{\sqrt{\| \mathbf{s} \|^2}}, \\ &p(\mathbf{T}_{ei}|K, S_{ci}, \sigma_d^2) = N(\mu_{ei}, (1-\rho)\sigma_d^2 \mathbf{I}_M), \\ &\text{with } \mu_{ei}(j) = \begin{cases} \frac{1-\rho}{K} \| \mathbf{s} \|, & \text{if } j \in S_{ci}, \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

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 (8) in Stage 2 now becomes

$$\hat{\mathbf{j}}_i = \arg \max_{j=1}^{M} \{\mathbf{T}_{ei}(j) \geq h\}. \qquad (11)$$

Now the threshold h is chosen such that

$$Pr\{T_{ei}(j) \geq h | j \notin S_{ci}\} = Q\left(\frac{h}{\sqrt{1-\rho}\sigma_d}\right) = \alpha_2, \qquad (12)$$

Note that h is a common threshold for different groups. Advantages of the process (11) are that components of the vector $\mathbf{T}_{ei}$ are independent and that the resulting variance is smaller than σ_d^2.

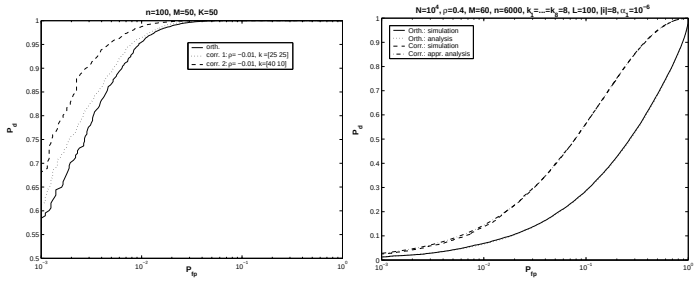
We proceed to evaluate the performance of the above system. Without loss of generality, we assume $\mathbf{i} = [1, 2, ..., l]$, where $\mathbf{i}$ indicates the indices of groups containing colluders. We have

$$\begin{aligned} P_{fp} &= Pr\{\cup_{i=1}^{L} A_i\} = [1 - (1-p_{l+1})^{L-l}] + \\ &\quad (1-p_{l+1})^{L-l} \sum_{i=1}^{l} p_i \Pi_{j=1}^{i-1}(1-p_j), \text{ with } p_i = Pr\{A_i\}. \\ P_d &= Pr\{\exists \hat{\mathbf{j}}_i \cap S_{ci} \neq \emptyset\} = Pr\{\cup_{i=1}^{l} B_i\}, \\ &= \sum_{i=1}^{l} q_i \Pi_{j=1}^{i-1}(1-q_j), \text{ with } q_i = Pr\{B_i\}. \qquad (13) \end{aligned}$$

with $A_i = \{T_G(i) \geq h_G, \max_{j \notin S_{ci}} T_{si}(j) \geq h_i\}$ and $B_i = \{T_G(i) \geq h_G, \max_{j \in S_{ci}} T_{si}(j) \geq h_i\}$, by utilizing the independency among fingerprints belonging to different groups. Based on this pair of criteria, the system requirements are represented as

$$P_{fp} \leq \epsilon; \quad P_d \geq \beta. \qquad (14)$$

We can see that the difficulty in analyzing the collusion resistance lies in calculating such joint probabilities as p_i and q_i. We first show the performance by examples when the total number of users is small and a negative $\rho = -0.01$ is used, as in Fig. 2(a). It is clear that introducing a negative ρ helps to improve the performance when n is small. It seems the worst case, in the sense of performance, happens when each guilty group contributes equal number of colluders, meaning $k_i = K/|\mathbf{i}|$, for $i \in \mathbf{i}$.



(a) (b)

Fig. 2. ROC curves P_d vs. P_{fp} of different examples, compared with the orthogonal scheme in [9]. In (a), a small number of users $n = 100$ and a negative $\rho = -0.01$ are considered. In (b), a large number of users $n = 6000$ and a positive $\rho = 0.4$ are considered.

We further note that the correlation between $T_G(i)$ and $T_{ei}(j)$ is equal to $\sqrt{\frac{1-\rho}{M+(M^2-M)\rho}}$, a small value close to 0. For instance, with $\rho = 0.2$ and $M = 60$, this correlation is as small as 0.03. It suggests us to assume that $T_G(i)$ and $T_{ei}(j)$'s are approximately uncorrelated, therefore we have the following approximation

$$\begin{aligned} p_i &\approx Pr\{T_G(i) \geq h_G\} Pr\{\max_{j \notin S_{ci}} T_{ei}(j) \geq h\} \qquad (15) \\ &= Q(\frac{h_G - k_i r}{\sigma_d}) \left[1 - (1 - Q(\frac{h}{\sqrt{1-\rho}\sigma_d}))^{M-k_i}\right], \\ q_i &\approx Q(\frac{h_G - k_i r}{\sigma_d}) \left[1 - (1 - Q(\frac{h - (1-\rho)\|\mathbf{s}\|/K}{\sqrt{1-\rho}\sigma_d}))^{k_i}\right], \end{aligned}$$

in calculating P_{fp} and P_d in (13), with $r = \frac{\|\mathbf{s}\|\sqrt{1+(M-1)\rho}}{K\sqrt{M}}$. As shown in Fig. 2(b), we note that this approximation is very accurate, and our scheme is superior to the orthogonal one.

To have an overall understanding of the collusion resistance of the proposed scheme, we further study the maximum resistable number of colluders K_{max} as a function of n. 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 affects the probability of group detection, are chosen to maximize $P_d(\alpha_1, \alpha_2, \rho)$ subject to the constraint $P_{fp}(\alpha_1, \alpha_2, \rho) \leq \epsilon$. In reality, the value of ρ is limited by the quantization precision of the image system. With the fact (at least with our hope) that the size $|\mathbf{i}|$ should be reasonable, we note that the results are not as sensitive to α_1 and ρ as to α_2. Therefore, to simplify our searching process, we discrete the values of α_1 and ρ. Also, we consider the performance of the worst case where $k_i = K/|\mathbf{i}|$, for $i \in \mathbf{i}$. We illustrate an example in Fig. 3, where $M = 60$ is used since it is proved to be the best supportable user size for the orthogonal scheme. 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. Overall, the group-based 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.

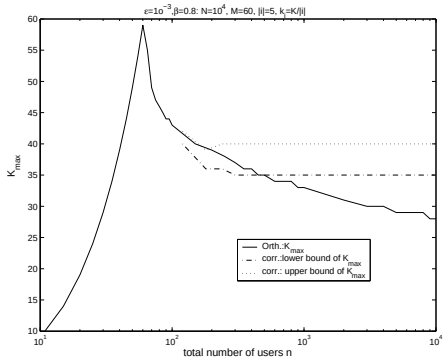


Fig. 3. Comparison of collusion resistance of the orthogonal and the proposed group-based fingerprinting systems to the average attack. Here $M = 60$, $k_i = K/|i|$, $|i| = 5$, and the system requirements are represented by $\epsilon = 10^{-3}$ and $\beta = 0.8$.

5. CONCLUSION

In this paper, we investigated how to improve the collusion resistance performance of fingerprinting systems using orthogonal modulations. We proposed a Gaussian fingerprinting system employing grouping and introduced equal correlations into fingerprints for users within the same group. We proposed a two-stage detection scheme and analyzed the collusion resistance of our fingerprinting system to the average attack under the performance criteria represented by P_{fp} and P_d. It was demonstrated that the proposed fingerprinting scheme is superior to orthogonal fingerprints, when the number of guilty groups is mild. In this work we assumed that the detector knew the number of colluders k_i from each group. However, this is typically not known in practice, and in the future we plan to investigate techniques for estimating k_i and studying the effect that using estimated k_i has upon detection performance.

6. REFERENCES

[1] D. Boneh and J. Shaw, "Collusion-Secure Fingerprinting for Digital Data", *IEEE Trans. on Information Theory*, Vol. 44, pp. 1897-1905, 1998.

[2] I. Cox, J. Bloom and M. Miller, *Digital Watermarking: Principles & Practice*, Morgan Kaufman Publishers, 2001.

[3] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Trans. on Image Proc.*, vol. 6, no. 12, pp. 1673-87, 1997.

[4] F. Ergun, J. Kilian and R. Kumar, "A Note on the limits of Collusion-Resistant Watermarks", *Proc. of Eurocrypt'99*, pp. 140-49, 1999.

[5] J. Kilian, T. Leighton, L. Matheson, T. Shamoon, R. Tarjan, and F. Zane, "Resistance of Digital Watermarks to Collusive Attacks", *Proc. of IEEE ISIT98*, pp. 271, Aug. 1998.

[6] J. Su, J. Eggers, and B. Girod, "Capacity of Digital Watermarks Subjected to An Optimal Collusion Attack", *Proc. of EUSIPCO2000*, 2000.

[7] H. Stone, "Analysis of Attacks on Image Watermarks with Randomized Coefficients", Tech. Rep. 96-045, NEC Research Institute, Princeton, NJ, 1996.

[8] W. Trappe, M. Wu, Z. Jane Wang and K. J. R. Liu, "Anti-Collusion Fingerprinting for Multimedia", *to appear IEEE Trans. on SP, Special issue on SP for Data Hiding in Digital Media & Secure Content Delivery*, Feb. 2003.

[9] Z. Jane Wang, M. Wu, H. Zhao, W. Trappe, and K. Ray Liu, "Collusion Resistance of Multimedia Fingerprinting Using Orthogonal Modulation",*to appear ICASSP2003*, Apr. 2003.