RESISTANCE ANALYSIS OF SCALABLE VIDEO FINGERPRINTING SYSTEMS UNDER FAIR COLLUSION ATTACKS

H. Vicky Zhao and K. J. Ray Liu

Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742

ABSTRACT

Digital fingerprinting is an important tool in multimedia forensics to trace traitors and protect multimedia content after decryption. This paper addresses the enforcement of digital rights when distributing multimedia over heterogeneous networks and studies the scalable multimedia fingerprinting systems in which users receive copies of different quality. We investigate the traitor tracing capability of such scalable fingerprinting systems, in particular, the robustness of the embedded fingerprints against multi-user collusion attacks. Under the fairness constraints on collusion that all attackers share the same risk of being captured, we analyze the maximum number of colluders that the fingerprinting systems can withstand, and our results show that multimedia fingerprints can survive collusion attacks by a few dozen colluders.

1. INTRODUCTION

With widespread distribution of multimedia, it is critical to secure multimedia content and enforce intellectual property rights. A fundamental problem in multimedia security and forensics is to identify entities involved in the illegal usage of multimedia. Digital fingerprinting embeds unique identification information in the content before distribution and can be used in traitor tracing.

The uniqueness of each distributed copy enables multiple attackers to collect several fingerprinted copies of the same content, mount attacks together, and remove the embedded fingerprints [1]. Such a *collusion* attack poses serious threats to digital fingerprinting systems. To enable traitor tracing and support multimedia forensics, it is important for the digital rights enforcer to understand the collusion attacks, analyze the collusion resistance of digital fingerprinting systems, and develop anti-collusion fingerprint codes. This paper focuses on the collusion resistance analysis that provides foundations for the collusion secure fingerprint design.

Multi-user collusion was modeled as averaging attack followed by an additive noise in [2], and it was shown that $O(\sqrt{N/\log N})$ colluders were enough to break the fingerprinting systems where N is the fingerprint length. Similar results were provided in [3]. The work in [4] evaluated the maximum number of colluders that digital fingerprinting systems can withstand and investigated the relationship between the collusion resistance and the fingerprint length, the total number of users, and the system requirements.

Most prior work on collusion attacks and fingerprint design for multimedia assumed that users receive copies of the same quality. In practice, *scalability* is often required during video transmission to address the heterogeneity of network and that of the end users. The impact of scalability on fingerprinting systems was studied in [5]. Their work analyzed the effectiveness of collusion attacks under the constraints that all colluders have equal probability of being detected. Based on the work in [5], this paper investigates the resistance of scalable fingerprinting systems against fair collusion attacks and analyzes the maximum number of colluders that are necessary to undermine the scalable fingerprinting systems.

This paper is organized as follows. We begin in Section 2 with the introduction of the scalable video coding systems and the scalable fingerprinting system model that are used in this paper. Section 3 analyzes the collusion resistance of the scalable fingerprinting systems. Section 4 shows the simulation results, and conclusions are drawn in Section 5.

2. SYSTEM MODEL

2.1. Temporally Scalable Video Coding Systems

To achieve scalability, we use layered video coding and decompose the content into non-overlapping parts of different priority. The base layer contains the most important information of the video and is received by all users. The enhancement layers gradually refine the reconstructed sequence and are only received by users with sufficient bandwidth. Without loss of generality, we consider a temporally scalable video coding system with three-layer scalability: the base layer has top priority, the enhancement layer 1 has medium priority, and the enhancement layer 2 has low priority. Same as in [5], we consider a simple implementation of the temporal scalability and encode different frames in different layers.[1] Define F_b, F_{e1} and F_{e2} as the sets containing indices of the frames that are encoded in the base layer, enhancement layer 1 and enhancement layer 2, respectively. For example, $F_b = \{1, 5, 9, \cdots\}$, $F_{e1} = \{3, 7, 11, \cdots\}$ and $F_{e2} = \{2, 4, 6, \cdots\}$.

Define $F^{(i)}$ as the set containing the indices of the frames that user $\mathbf{u}^{(i)}$ receives from the content owner. We further define $\mathbf{U}^b \triangleq \{\mathbf{u}^{(i)} : F^{(i)} = F_b\}$ as the subgroup of users who receive the base layer only; $\mathbf{U}^{b,e1} \triangleq \{\mathbf{u}^{(i)} : F^{(i)} = F_b \cup F_{e1}\}$ is the subgroup of users who receive the base layer and enhancement layer 1; and $\mathbf{U}^{all} \triangleq \{\mathbf{u}^{(i)} : F^{(i)} = F_b \cup F_{e1} \cup F_{e2}\}$ is the subgroup of users who receive all three layers. $M = |\mathbf{U}^b| + |\mathbf{U}^{b,e1}| + |\mathbf{U}^{all}|$ is the total number of users, where $|A|$ returns the size of the set A.

2.2. Digital Fingerprinting System Model

A digital fingerprinting system usually contains three parts: fingerprint embedding, collusion attacks, and fingerprint detection.

Fingerprint Embedding With the above temporally scalable cod-

The authors can be reached at hzhao and kjrliu@eng.umd.edu.

[1] For example, with MPEG-2 video coding, the base layer may contain all the I frames, the enhancement layer 1 contains all the P frames, and the enhancement layer 2 contains all the B frames.

0-7803-9134-9/05/$20.00 ©2005 IEEE

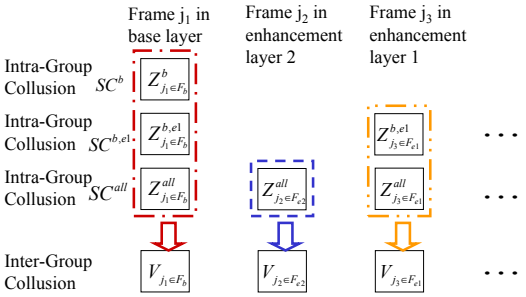


Fig. 1. The intra-group and inter-group collusion attacks.

ing systems, for the jth frame in the video represented by a vector $\mathbf{S}_j$ of length N_j, and for each user $\mathbf{u}^{(i)}$ who subscribes to frame j, the content owner generates a unique fingerprint $\mathbf{W}_j^{(i)}$ of length N_j. The fingerprinted frame j that will be distributed to $\mathbf{u}^{(i)}$ is $\mathbf{X}_j^{(i)} = \mathbf{S}_j + JND_j \cdot \mathbf{W}_j^{(i)}$. JND here is the just-noticeable-difference from human visual models [6] to control the energy of the embedded fingerprints. Finally, the content owner transmits to $\mathbf{u}^{(i)}$ all the fingerprinted frames that he subscribes to.

In this paper, we use Gaussian distributed fingerprints and generate $\{\mathbf{W}_j^{(i)}\}$ from distribution $\mathcal{N}(0, \sigma_W^2)$. To be robust against intra-content collusion attacks by a single adversary, similar to [7], in each distributed copy, we embed correlated fingerprints into adjacent frames and let the correlation depend on the similarity between the two host frames. In this paper, fingerprints for different users are generated independently.

Collusion Attacks During collusion, the colluders collect all the received fingerprinted copies and apply multi-user collusion to attenuate the embedded fingerprints. It was shown in [4] that if all collusion attacks generate colluded copies of the same quality, nonlinear collusion attacks have approximately the same performance as the averaging based collusion. Thus, we only consider averaging based collusion in this paper.

Given that the attackers receive copies of different quality due to network heterogeneity, this paper assumes that the colluders wish to generate colluded copies of high resolution and good quality under the constraints that every colluder has the same probability of being captured. Following the work in [5], the colluders first divide themselves into three non-overlapping subgroups:

- $SC^b \triangleq \{i : F^{(i)} = F_b\}$ contains the indices of colluders who receive the base layer only;
- $SC^{b,e1} \triangleq \{i : F^{(i)} = F_b \cup F_{e1}\}$ contains the indices of colluders who receive base layer and enhancement layer 1;
- and $SC^{all} \triangleq \{i : F^{(i)} = F_b \cup F_{e1} \cup F_{e2}\}$ contains the indices of colluders who receive all three layers.

Define K^b, $K^{b,e1}$, and K^{all} as the number of colluders in subgroups SC^b, $SC^{b,e1}$, and SC^{all}, respectively. Then, the colluders apply the intra-group collusion attacks:

- For each frame $j \in F_b$ that they received, the colluders in the subgroup SC^b generate $\mathbf{Z}_j^b = \sum_{i \in SC^b} \mathbf{X}_j^{(i)} / K^b$.
- For each frame $j \in F_b \cup F_{e1}$ that they received, the colluders in $SC^{b,e1}$ generate $\mathbf{Z}_j^{b,e1} = \sum_{i \in SC^{b,e1}} \mathbf{X}_j^{(i)} / K^{b,e1}$.
- For each frame $j \in F_b \cup F_{e1} \cup F_{e1}$ that they received, the colluders in SC^{all} generate $\mathbf{Z}_j^{all} = \sum_{i \in SC^{all}} \mathbf{X}_j^{(i)} / K^{all}$.

Define F^c as the set containing indices of the frames in the colluded copy $\{\mathbf{V}_j\}$. $F^c = F_b$, $F^c = F_b \cup F_{e1}$, and $F^c = F_b \cup F_{e1} \cup F_{e2}$ correspond to the three scenarios where $\{\mathbf{V}_j\}$ has the lowest, medium, and highest resolutions, respectively. Finally, the colluders apply the inter-group collusion as shown in Figure 1:

- For each frame $j \in F_b$ in the base layer, $\mathbf{V}_j = \beta_1 \mathbf{Z}_j^b + \beta_2 \mathbf{Z}_j^{b,e1} + \beta_3 \mathbf{Z}_j^{all} + \mathbf{n}_j$, where $\beta_1 + \beta_2 + \beta_3 = 1$ and $0 \le \beta_1,\ \beta_2,\ \beta_3 \le 1$. $\mathbf{n}_j$ is an additive noise.
- If $F_{e1} \subset F^c$ and the colluded copy contains frames in the enhancement layers, then for each frame $j \in F_{e1}$ in the enhancement layer 1, $\mathbf{V}_j = \alpha_1 \mathbf{Z}_j^{b,e1} + \alpha_2 \mathbf{Z}_j^{all} + \mathbf{n}_j$, where $0 \le \alpha_1,\ \alpha_2 \le \alpha_1 + \alpha_2 = 1$ and $\mathbf{n}_j$ is an additive noise.
- If $F_{e2} \subset F^c$ and the colluded copy contains all the frames, then for each frame $j \in F_{e2}$ in the enhancement layer 2, $\mathbf{V}_j = \mathbf{Z}_j^{all} + \mathbf{n}_j$, where $\mathbf{n}_j$ is an additive noise.

To address the fairness issue during collusion and ensure that all attackers have the same risk of being detected, Table 1 lists the constraints and the selection of the parameters, F^c, $\{\beta_k\}$, and $\{\alpha_l\}$, to achieve the fairness of collusion [5]. In Table 1, N_b, N_{e1}, and N_{e2} are the lengths of the fingerprints embedded in the base layer, enhancement layer 1 and enhancement layer 2, respectively.

Fingerprint Detection In digital fingerprinting applications, the host signal can be made available to the detector. We consider a non-blind detection scenario where the host signal is first removed from the test copy before colluder identification. The detector first extracts the fingerprint $\mathbf{Y}_j$ from the jth frame $\mathbf{V}_j$ in the colluded copy, measures the similarity between the extracted fingerprint and each of the original fingerprints, compares with a threshold h, and outputs the estimated identities of the colluders $\widehat{SC}$.

We consider a simple detector that collectively uses fingerprints extracted from all layers to identify colluders. For each user $\mathbf{u}^{(i)}$, the detector first calculates $\breve{F}^{(i)} \triangleq F^{(i)} \cap F^c$, where $F^{(i)}$ contains the indices of frames received by $\mathbf{u}^{(i)}$ and F^c contains the indices of frames in the colluded copy. Then the detector calculates

$$T_N^{(i)} = \left(\sum_{j \in \breve{F}^{(i)}} \langle \mathbf{Y}_j, \mathbf{W}_j^{(i)} \rangle \right) / \sqrt{\sum_{j \in \breve{F}^{(i)}} ||\mathbf{W}_j^{(i)}||^2}, \quad (1)$$

where $||\mathbf{W}_j^{(i)}||$ is the Euclidean norm of $\mathbf{W}_j^{(i)}$. Given a predetermined threshold h, $\widehat{SC} = \{i : T_N^{(i)} > h\}$.

2.3. System Requirements and Performance Criteria

Digital fingerprints can be used in various applications with different requirements [4]. In this paper, we take the *catch one* scenario as an example, and the analysis for other scenarios are similar. In the catch one scenario, the goal is to maximize the chance to capture one colluder without accusing any innocents, and the performance criteria are the probability of capturing at least one colluder (P_d) and the probability of accusing at least one innocent user (P_{fp}). Under the system requirements that $P_d \ge \gamma_d$ and $P_{fp} \le \gamma_{fp}$, we analyze the maximum number of colluders (K_{max}) that the scalable fingerprinting systems can resist.

3. COLLUSION RESISTANCE ANALYSIS

3.1. Analysis of P_d and P_{fp}

To analyze K_{max}, we need to calculate P_d and P_{fp} first. From [5], if the colluders choose the collusion parameters as in Table 1, for

Table 1. Fairness Constraints on Collusion Attacks and The Selection of Collusion Parameters.

$F^c = F_b \cup F_{e1} \cup F_{e2}$	Fairness Constraints	$\begin{cases} \frac{K^b\sqrt{N_b}}{K^b\sqrt{N_b}+K^{b,e1}\sqrt{N_b+N_{e1}}+K^{all}\sqrt{N_b+N_{e1}+N_{e2}}} \le \frac{N_b}{N_b+N_{e1}+N_{e2}}, \\ \frac{K^{all}\sqrt{N_b+N_{e1}+N_{e2}}}{K^b\sqrt{N_b}+K^{b,e1}\sqrt{N_b+N_{e1}}+K^{all}\sqrt{N_b+N_{e1}+N_{e2}}} \ge \frac{N_{e2}}{N_b+N_{e1}+N_{e2}}. \end{cases}$
	Parameter Selection	$\begin{cases} \beta_1 = \frac{N_b+N_{e1}+N_{e2}}{N_b} \frac{K^b\sqrt{N_b}}{K^b\sqrt{N_b}+K^{b,e1}\sqrt{N_b+N_{e1}}+K^{all}\sqrt{N_b+N_{e1}+N_{e2}}}, \\ \beta_2 N_b + \alpha_1 N_{e1} = \frac{(N_b+N_{e1}+N_{e2})K^{b,e1}\sqrt{N_b+N_{e1}}}{K^b\sqrt{N_b}+K^{b,e1}\sqrt{N_b+N_{e1}}+K^{all}\sqrt{N_b+N_{e1}+N_{e2}}}, \\ \beta_3 = 1-\beta_1-\beta_2,\ \alpha_2 = 1-\alpha_1. \end{cases}$
$F^c = F_b \cup F_{e1}$	Fairness Constraints	$\frac{K^b\sqrt{N_b}}{K^b\sqrt{N_b}+(K^{b,e1}+K^{all})\sqrt{N_b+N_{e1}}} \le \frac{N_b}{N_b+N_{e1}}$.
	Parameter Selection	$\begin{cases} \beta_1 = \frac{N_b+N_{e1}}{N_b} \frac{K_b\sqrt{N_b}}{K^b\sqrt{N_b}+(K^{b,e1}+K^{all})\sqrt{N_b+N_{e1}}}, \\ \beta_2 = \frac{K^{b,e1}}{K^{b,e1}+K^{all}}(1-\beta_1),\ \beta_3 = 1-\beta_1-\beta_2, \\ \alpha_1 = \frac{K^{b,e1}}{K^{b,e1}+K^{all}},\ \alpha_2 = 1-\alpha_1. \end{cases}$
$F^c = F_b$	Fairness Constraints	No constraints on $(K^b, K^{b,e1}, K^{all})$ and (N_b, N_{e1}, N_{e2}).
	Parameter Selection	$\beta_1 = \frac{K^b}{K^b+K^{b,e1}+K^{all}},\ \beta_2 = \frac{K^{b,e1}}{K^b+K^{b,e1}+K^{all}},\ \beta_3 = \frac{K^{all}}{K^b+K^{b,e1}+K^{all}}$.

user $\mathbf{u}^{(i)}$, the detection statistics follow Gaussian distribution

$$p(T_N^{(i)}|SC) \sim \begin{cases} \mathcal{N}(\mu,\ \sigma_n^2) & \text{if } i \in SC, \\ \mathcal{N}(0,\ \sigma_n^2) & \text{if } i \notin SC, \end{cases} \tag{2}$$

where σ_n^2 is the variance of the additive noise $\mathbf{n}_j$ and

$$\mu \approx \begin{cases} \frac{N_b+N_{e1}+N_{e2}}{K^b\sqrt{N_b}+K^{b,e1}\sqrt{N_b+N_{e1}}+K^{all}\sqrt{N_b+N_{e1}+N_{e2}}}\sigma_W \\ \qquad \text{if } F^c = F_b \cup F_{e1} \cup F_{e2}, \\ \frac{N_b+N_{e1}}{K^b\sqrt{N_b}+(K^{b,e1}+K^{all})\sqrt{N_b+N_{e1}}}\sigma_W \quad \text{if } F^c = F_b \cup F_{e1}, \\ \frac{\sqrt{N_b}}{K^b+K^{b,e1}+K^{all}}\sigma_W \qquad \text{if } F^c = F_b. \end{cases} \tag{3}$$

The M detection statistics $\{T_N^{(i)}\}_{i=1}^M$ are independent of each other. Given the threshold h, we can have the approximation that

$$P_d \approx 1-[1-Q(\frac{h-\mu}{\sigma_n})]^K \text{ and } P_{fp} \approx 1-[1-Q(\frac{h}{\sigma_n})]^{M-K}, \tag{4}$$

where $Q(\cdot)$ is the Gaussian tail function.

3.2. Upper and Lower Bounds of K_{max}

Define $K = K^b + K^{b,e1} + K^{all}$ as the total number of colluders. From (2)-(4), for a fixed K, the performance of the scalable fingerprinting system depends on the resolution of the colluded copy: its performance is better when the colluded copy has higher resolution and better quality. This is because when there are more frames in the colluded copy, the extracted fingerprint is longer and gives the detector more information of the colluders' identities.

Given $(|\mathbf{U}^b|, |\mathbf{U}^{b,e1}|, |\mathbf{U}^{all}|)$, (N_b, N_{e1}, N_{e2}), γ_{fp}, and the total number of colluders K, we define

$$\begin{aligned} & P_d^U(K) \stackrel{\triangle}{=} \max_{F^c,(K^b,K^{b,e1},K^{all})} P_d, \\ s.t. \quad & K^b + K^{b,e1} + K^{all} = K,\ 0 \le K^b \le |\mathbf{U}^b|, \\ & 0 \le K^{b,e1} \le |\mathbf{U}^{b,e1}|,\ 0 \le K^{all} \le |\mathbf{U}^{all}|, \\ & \text{fairness constraints in Table 1 are satisfied;} \end{aligned} \tag{5}$$

and

$$\begin{aligned} & P_d^L(K) \stackrel{\triangle}{=} \min_{F^c,(K^b,K^{b,e1},K^{all})} P_d, \\ s.t. \quad & K^b + K^{b,e1} + K^{all} = K,\ 0 \le K^b \le |\mathbf{U}^b|, \\ & 0 \le K^{b,e1} \le |\mathbf{U}^{b,e1}|,\ 0 \le K^{all} \le |\mathbf{U}^{all}|, \\ & \text{fairness constraints in Table 1 are satisfied.} \end{aligned} \tag{6}$$

For a fixed K, $P_d^U(K)$ and $P_d^L(K)$ are the upper and lower bounds of P_d, respectively. We further define

$$\begin{aligned} K_{max}^U & \stackrel{\triangle}{=} \arg_K\{P_d^U(K) \ge \gamma_d,\ P_d^U(K+1) < \gamma_d\} \\ \text{and } K_{max}^L & \stackrel{\triangle}{=} \arg_K\{P_d^L(K) \ge \gamma_d,\ P_d^L(K+1) < \gamma_d\} \end{aligned} \tag{7}$$

which are the upper and lower bounds of K_{max}, respectively. When the total number of colluders K is smaller than K_{max}^L, the system requirements are always satisfied no matter what values F^c and $(K^b, K^{b,e1}, K^{all})$ take. If K is larger than K_{max}^U, for all possible values of F^c and $(K^b, K^{b,e1}, K^{all})$, the detector will always fail under the system requirements $P_d \ge \gamma_d$ and $P_{fp} \le \gamma_{fp}$.

3.3. Analysis of K_{max}^U and K_{max}^L

To calculate K_{max}^U and K_{max}^L, we first need to calculate $P_d^U(K)$ and $P_d^L(K)$. From (3) and (4), for a given K, the lower bound of P_d is achieved when the colluded copy contains frames in the base layer only, i.e., $F^c = F_b$, and $\mu = \sqrt{N_b}\sigma_W/K$. Consequently,

$$P_d^L(K) \approx 1-[1-Q(\frac{h-\sqrt{N_b}\sigma_W/K}{\sigma_n})]^K. \tag{8}$$

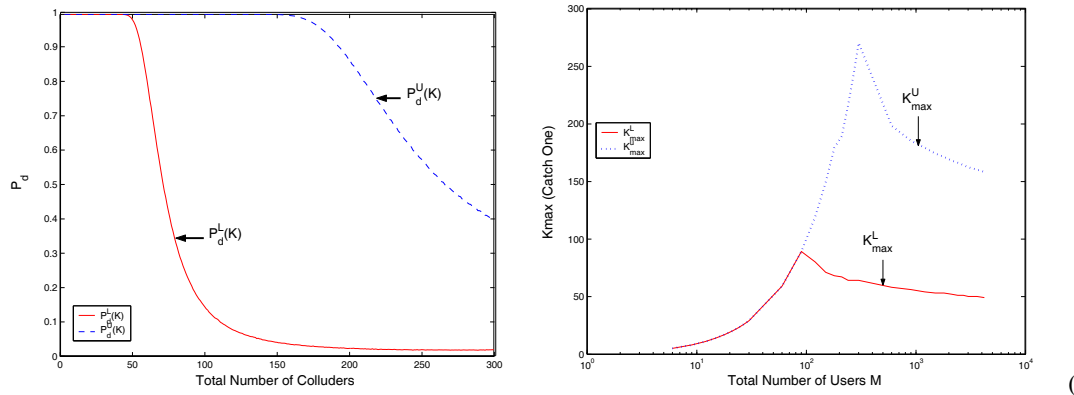
To calculate $P_d^U(K)$, we observe that the upper bound of P_d is achieved when the colluded copy has the highest possible resolution under the fairness constraints. From (3) and (4), with fixed K, maximizing P_d is equivalent to maximizing μ in (3) under the fairness constraints. Thus, the problem of (5) can be simplified to

$$\begin{aligned} & \mu^U(K) \stackrel{\triangle}{=} \max_{F^c,(K^b,K^{b,e1},K^{all})} \mu, \\ s.t. \quad & K^b + K^{b,e1} + K^{all} = K,\ 0 \le K^b \le |\mathbf{U}^b|, \\ & 0 \le K^{b,e1} \le |\mathbf{U}^{b,e1}|,\ 0 \le K^{all} \le |\mathbf{U}^{all}|, \\ & \text{fairness constraints in Table 1 are satisfied.} \end{aligned} \tag{9}$$

We use linear programming [8] to solve the problem of (9), and detailed analysis is available in [9]. With $\mu^U(K)$ as in (9),

$$P_d^U(K) \approx 1-[1-Q(\frac{h-\mu^U(K)}{\sigma_n})]^K. \tag{10}$$

Given $P_d^L(K)$ as in (8) and $P_d^U(K)$ as in (10), the analysis of K_{max}^L and K_{max}^U is the same as that in [4] and not repeated here.



(a) (b)

Fig. 2. Simulation results of the collusion resistance in the catch one scenario. $|\mathbf{U}^b| : |\mathbf{U}^{b,e1}| : |\mathbf{U}^{all}| = 1 : 1 : 1$ and $(N_b, N_{e1}, N_{e2}) = (50000, 50000, 100000)$. $\gamma_d = 0.8$ and $\gamma_{fp} = 10^{-3}$. (a) shows $P_d^U(K)$ and $P_d^L(K)$ versus the total number of colluders K when $M = 450$ and $|\mathbf{U}^b| = |\mathbf{U}^{b,e1}| = |\mathbf{U}^{all}| = 150$. (b) illustrates K_{max}^U and K_{max}^L versus the total number of users M.

4. SIMULATION RESULTS

In our simulations, we adopt the human visual model based spread spectrum embedding [6] and embed fingerprints in the DCT domain. The fingerprints follow Gaussian distribution $\mathcal{N}(0, 1/9)$, and fingerprints for different users are generated independently. In each distributed copy, similar to the work in [7], correlated fingerprints are embedded into adjacent frames, and the correlation depends on the similarity between the host frames.

For real video sequences like "miss america" and "carphone", the number of embeddable coefficients in each frame varies from 3000 to 7000, depending on the characteristics of the video. In our simulations, we assume that the lengths of the fingerprints embedded in each frame is approximately 5000, and we test on a total of 40 frames. We choose $F_b = \{1, 5, 9, \cdots\}$, $F_{e1} = \{3, 7, 11, \cdots\}$ and $F_{e2} = \{2, 4, 6, 8, \cdots\}$ as an example of the temporal scalability, and the lengths of the fingerprints embedded in the base layer, enhancement layer 1, and enhancement layer 2 are $N_b = 50000$, $N_{e1} = 50000$, and $N_{e2} = 100000$, respectively.

During collusion, for simplicity, we assume that the collusion attack is also in the DCT domain and the colluders apply the two-stage collusion attack as in Section 2.2. For each frame in the colluded copy, we adjust the power of the additive noise such that $||\mathbf{n}_j||^2/||\mathbf{W}_j^{(i)}||^2 = 2$, and other values will give the same trend.

We consider the non-blind detection and remove the host signal from the test copy before detection. The detector then applies the detection process in Section 2.2 to identify the colluders.

Figure 2 (a) shows $P_d^U(K)$ and $P_d^L(K)$ versus the total number of colluders when there are a total of $M = 450$ users and $\gamma_{fp} = 10^{-3}$. From Figure 2 (a), when $K \geq 210$, $P_d^U(K) < 0.8$ and the fingerprinting systems will always fail; and when $K \leq 60$, $P_d^L(k) \geq 0.8$ and the colluders can never bypass the detector without being detected. Figure 2 (b) plots the K_{max}^L and K_{max}^U versus the total number of users when $\gamma_d = 0.8$ and $\gamma_{fp} = 10^{-3}$. From the attackers' point of view, if they manage to collect more than K_{max}^U copies, they can be guaranteed success even if they generate a colluded copy of the highest resolution and best quality. From the content owner's point of view, if he/she can ensure that potential colluders cannot collect more than K_{max}^L copies, the fingerprinting system is essentially collusion resistant.

From Figure 2 (b), for applications with thousands of users, the fingerprinting system can withstand approximately 50 colluders. Furthermore, if the content owner distributes no more than 100 copies, the detection performance will always satisfy the requirement even if all users participate in collusion. Consequently, the fingerprinting system is also collusion-secure if $M \leq 100$.

5. CONCLUSIONS

In this paper, we have studied scalable fingerprinting systems in which users receive copies of different quality and investigated their resistance against collusion attacks. We have shown that the scalable fingerprinting systems can resist up to a few dozen colluders. We have also analyzed the lower and upper bounds of K_{max}. From the colluders' point of view, K_{max}^U tells them the number of copies necessary to guarantee the success of collusion under all circumstances. From the content owner's point of view, to achieve collusion free, a desired security requirement is to make the potential colluders unlikely to collect more than K_{max}^L copies.

6. REFERENCES

[1] H. Stone, "Analysis of attacks on image watermarks with randomized coefficients," Tech. Rep. 96-045, NEC Research Institute, 1996.

[2] F. Zane, "Efficient watermark detection and collusion security," *Proc. of Financial Cryptography, Lecture of Notes in Computer Science*, vol. 1962, pp. 21–32, Feb. 2000.

[3] F. Ergun, J. Killian, and R. Kumar, "A note on the limits of collusion-resistant watermarks," *Advances in Cryptology – EuroCrypto '99, Lecture Notes in Computer Science*, vol. 1592, pp. 140–149, 2001.

[4] Z. J. Wang, M. Wu, H. Zhao, W. Trappe, and K. J. R. Liu, "Resistance of orthogonal gaussian fingerprints to collusion attacks," *IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, April 2003.

[5] H. Zhao and K. J. R. Liu, "Fair collusion attacks on scalable video fingerprinting systems," *IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, vol. II, pp. 1045–1048, March 2005.

[6] C. Podilchuk and W. Zeng, "Image adaptive watermarking using visual models," *IEEE Journal on Sel. Area in Comm.*, vol. 16, no. 4, pp. 525–540, May 1998.

[7] K. Su, D. Kundur, and D. Hatzinakos, "Statistical invisibility for collusion-resistant digital video watermarking," *IEEE Tran. on Multimedia*, vol. 7, no. 1, pp. 43–51, Feb. 2005.

[8] G. Dantzig, *Linear Programming and Extensions*, Princeton University Press, 1963.

[9] H. Zhao and K. J. R. Liu, "Multimedia forensics for multi-user collusion on scalable fingerprinting systems: Fairness and effectiveness," *submitted to IEEE Tran. on Information Forensics and Security*.