A GAME THEORETIC FRAMEWORK FOR COLLUDER-DETECTOR BEHAVIOR FORENSICS

W. Sabrina Lin[*], *H. Vicky Zhao*[†] *and K. J. Ray Liu*[*]

[*] ECE Dept., University of Maryland, College Park, MD 20742 USA
[†] ECE Dept., University of Alberta, Edmonton, AB T6G 2V4 Canada

ABSTRACT

Digital fingerprinting is an emerging technology in media security to identify the source of illicit copies and trace traitors. Collusion is a powerful attack, in which a group of attacker collectively mount attacks against digital fingerprinting. In multimedia fingerprinting, there exists complex dynamics between the colluders and the fingerprint detector, who have conflicting objectives and influence each other's performance and decisions. This paper proposes a game-theoretic framework to formulate and analyze the colluder-detector dynamics, in an effort to understand its impact on the traitor tracing performance of multimedia fingerprints. We investigate how colluders adjusts the collusion attacks to minimize their risk under the fairness constraint; and study how the fingerprint detector adapts his/her detection strategy accordingly to improve the collusion resistance, which is shown to be the min-max solution.

Index Terms— Multimedia forensics, security, game theory

1. INTRODUCTION

Digital fingerprinting is an emerging forensic tool to protect multimedia from unauthorized redistribution and illegal alteration. The "fingerprint" is an unique label that is embedded into every distributed copy to protectively trace the usage of multimedia data. Multi-user collusion is a powerful attack against digital fingerprinting, where a group of attackers work together to undermine the tracing capability. To provide reliable traitor tracing and support multimedia forensics, multimedia fingerprints should resist multi-user collusion as well as single-copy attacks and common signal processing. There has been a lot of work on anti-collusion fingerprint design [1–3], where techniques from different disciplines were applied to resist collusion.

In multimedia fingerprinting, the colluders and the fingerprint detector have conflicting objectives. The colluders try all their means to remove the identifying fingerprints in their copies; while the fingerprint detector wishes to be able to successfully capture colluders under all circumstances. They influence each other's performance and decisions, and there exists complex dynamics between the colluders and the fingerprint detector. It's crucial to formulate this dynamics and understand how the colluders and the fingerprint detector interact with and respond to each other. From the traitor tracing perspectively, such investigation helps to have a better understanding of multimedia forensics and improve the collusion resistance.

This paper studies the game-theoretic formulation and analysis of the dynamics between the colluders and the fingerprint detector. We model it as a two-stage, two-person zero-sum game, where the colluders try to minimize their probability of being detected under the constraint that they share the same risk; while the fingerprint detector probes side information of collusion and adjusts the detection strategy to maximize the traitor tracing capability.We also analyze whether there exists such a min-max solution for the colluders, and investigate how to reach the solution.

The rest of the paper is as follows. We begin in Section 2 with the introduction of the system model. Section 3 formulates the dynamics between the colluders and the detector using a game-theoretic framework, and Section 4 analyzes the existence of the min-max solution of this game. We show simulation results in Section 5, and conclusions are drawn in Section 6.

2. SYSTEM MODEL

2.1. Scalable Video Coding

As we move to the digital era and experience the convergence of network, communications and multimedia, scalability in multimedia coding becomes increasingly important for rich media access from anywhere by anyone [4]. It encodes multimedia into several bit streams (or layers) of different priorities: the base layer contains the most important information and must be received by all users; while the enhancement layers refine the resolution of the receiver's reconstructed copy and have lower priorities. Such an encoding structure provides flexible solutions for multimedia transmission and offers adaptivity to heterogeneous networks, varying channel conditions, and diverse computing capability at the receiving terminals.

Following the work in [5], we consider a temporally scalable video coding system, which encodes different frames in the video sequence in three different layers. Define F_b, $F_{b,e1}$ 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. $F^{(i)}$ includes the indices of the frames in the copy that user $\mathbf{u}^{(i)}$ receives. U^b is the subgroup of users who receive the base layer only; $U^{b,e1}$ contains all users who subscribe to the medium-resolution version with the base layer and the enhancement layer 1; and U^{all} contains the indices of the users who receive all three layers.

2.2. Scalable Multimedia Fingerprinting Forensic System

Fingerprint Embedding Given a frame $\mathbf{S}_j$ in the video sequence, for each user $\mathbf{u}^{(i)}$ who subscribes to that frame, the content owners generates a unique fingerprint $\mathbf{W}_j^{(i)}$ of the same length as $\mathbf{S}_j$, and additively embeds it into the host signal using spread spectrum embedding [6,7]. The fingerprinted frame is $\mathbf{X}_j^{(i)} = \mathbf{S}_j + JND_j\mathbf{W}_j^{(i)}$, where JND is from human visual models to make $\mathbf{X}_j^{(i)}$ be perceptually the same as the original host frame $\mathbf{S}_j$. We generate independent vectors from Gaussian distribution $\mathcal{N}(0, \sigma_W^2)$, and then apply Gram-Schmidt orthogonalization to generate orthogonal fingerprints.

Multi-user Collusion Let SC^b be the set of the indices of the colluders who receive the base layer only; $SC^{b,e1}$ contains the indices of the colluders who subscribe to the medium resolution copy; and SC^{all} contains the indices of colluders who receive all three layers. $K^b = |SC^b|$, $K^{b,e1} = |SC^{b,e1}|$ and $K^{all} = |SC^{all}|$, and $K = K^b + K^{b,e1} + K^{all}$ is the total number of colluders.

Following the two-stage collusion model in [5], during intra-group collusion, for each frame $j \in F_b$ in the base layer, collud-

ers in SC^b first generate $\mathbf{Z}_j^b = \sum_{k\in SC^b} \mathbf{X}_j^{(k)}/K^b$; for each frame $j \in F_b \cup F_{e1}$ that they receive, colluders in $SC^{b,e1}$ calculate $\mathbf{Z}_j^{b,e1} = \sum_{k\in SC^{b,e1}} \mathbf{X}_j^{(k)}/K^{b,e1}$; and for every frame in the video sequence, the colluders in SC^{all} generates $\mathbf{Z}_j^{all} = \sum_{k\in SC^{all}} \mathbf{X}_j^{(k)}/K^{all}$. Then, colluders apply inter-group collusion: for each frame $j \in F_b$ in the base layer, the colluded frame is $\mathbf{V}_j = \beta_1\mathbf{Z}_j^b + \beta_2\mathbf{Z}_j^{b,e1} + +(1-\beta_1-\beta_2)\mathbf{Z}_j^{all} + \mathbf{n}_j$, where $0 \le \beta_1, \beta_2, 1-\beta_1-\beta_2 \le 1$; for each frame $j_2 \in F_{e1}$ in the enhancement layer 1, $\mathbf{V}_{j_2} = \alpha_1\mathbf{Z}_{j_2}^{b,e1} + (1-\alpha_1)\mathbf{Z}_{j_2}^{all} + \mathbf{n}_{j_2}$ where $0 \le \alpha_1 \le 1$; and for each frame $j_3 \in F_{e2}$ in the enhancement layer 2, $\mathbf{V}_{j_3} = \mathbf{Z}_{j_3}^{all} + \mathbf{n}_{j_3}$. $\mathbf{n}_j$ is an additive noise to further hinder detection.

Fingerprint Detection At the detector's side, the fingerprint detector first removes the host signal $\mathbf{S}_j$ from the test copy $\mathbf{V}_j$ and extracts the fingerprint $\mathbf{Y}_j = (\mathbf{V}_j - \mathbf{S}_j)/JND_j$. Then, for each user, the fingerprint detector measures the similarity between the extracted fingerprint and the originally embedded fingerprint, compares with a threshold h and outputs the estimated colluder set.

Performance Criteria The commonly used criteria to evaluate a fingerprinting system's traitor tracing capability are: the probability of catching at least one colluder (P_d), and the probability of accusing at least one innocent user (P_{fp}).

3. COLLUDER-DETECTOR BEHAVIOR DYNAMICS

In this "cat-and-mouse" game between the attackers and the digital rights enforcer, colluders adjust the collusion attacks to minimize their chance of being detected under the constraint that they have equal risk; and the fingerprint detector adaptively select the detection strategy to maximize his/her success rate of capturing colluders.

Colluder Identification with Side Information To improve the detection performance, the work in [8] proposed a method to probe side information and explore unique features of collusion when identifying fingerprints. One candidate of such side information is the mean of the detection statistics that are used to measure the similarity between the extracted fingerprint and the original ones.

Take user $i \in \mathbf{U}^{all}$ who receives all three layers as an example, to measure the similarity between $\mathbf{Y}$ and $\mathbf{W}^{(i)}$, the fingerprint detector calculates

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

For the simple collective detector in [5], $\breve{F}^{(i)} = F_b \cup F_{e1} \cup F_{e2}$ and fingerprints extracted from all frames are used collectively to identify colluders. The fingerprint detector can also examine fingerprints extracted from each individual layer to identify colluders. For example, $\breve{F}^{(i)} = F_b$ if only fingerprints extracted from the base layer are used to decide whether $i \in SC$.

To determine whether user $i \in \mathbf{U}^{all}$ is a colluder, the fingerprint detector has four choices $\breve{F}^{(i)} \in \{F_b \cup F_{e1} \cup F_{e2}, F_b, F_{e1}, F_{e2}\}$, and thus four different statistics to measure the similarity between $\mathbf{Y}$ and $\mathbf{W}^{(i)}$. From the analysis in [8], the four detection statistics follow Gaussian distribution with the same variance but different means, and the one with the largest mean gives the best traitor tracing performance. Thus, the fingerprint detector should probe information about collusion and adapts its detection strategy accordingly to improve the collusion resistance. The work in [8] proposed a method for the fingerprint detector to estimate these means, and showed that the performance of this self-probing detector is almost the same as that of the optimum detector, who has perfect knowledge of the detection statistics' means and always selects the one with the best detection performance.

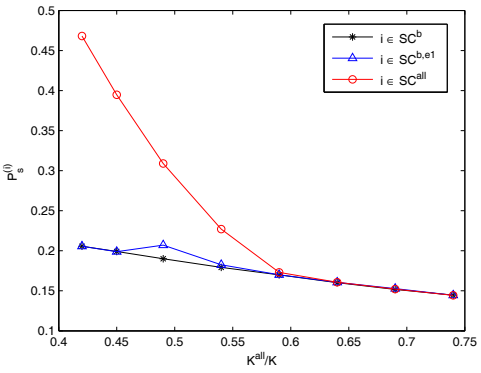


Fig. 1. Each colluder's probability of being detected ($P_s^{(i)}$) with the self-probing fingerprint detector. $(N_b, N_{e1}, N_{e2}) = (50000, 50000, 100000)$. $K = 250$. Each point on the x axis corresponds to a unique triplet $(K^b, K^{b,e1}, K^{all})$ where $K^b = 50$ and $K^{b,e1} = K - K^b - K^{all}$. Colluders follow [5] to select the collusion parameters $\{\alpha_j, \beta_l\}$. The threshold h is selected to satisfy $P_{fp} = 10^{-3}$. The results are based on 10000 simulation runs.

Side information about collusion not only improves the fingerprint detector's performance, it also affects each colluder's probability of being detected and influences how attackers collude. Take Figure 1 as an example, with the self-probing fingerprint detector, improper selection of the collusion parameters may make some colluders take a much higher risk than the others. Thus, having knowledge of what actions the fingerprint detector might take, colluders have to adjust the collusion attacks accordingly to minimize their risk and ensure the equal risk of all colluders.

A Game-Theoretic Framework We use game theory [9] to formulate this complex dynamics between the colluders and the fingerprint detector. This game involves two players, the colluders acting as one single player and the fingerprint detector. They have pure conflicting objectives and one player's gain is another's loss. Therefore, we can model this dynamics as a two-stage zero-sum game, where the colluders act first followed by the fingerprint detector.

In our game-theoretic framework, a natural and straightforward definition of the payoff function is the fingerprint detector's chance of successfully capturing the colluders, or equivalently, the colluders' risk of being detected. We use $P_s^{(i)}$, which is colluder $\mathbf{u}^{(i)}$'s probability of being detected.

Since the self-probing fingerprint detector has almost the same performance as the optimum detector, and this information is assumed to be known by the colluders, the colluders should assume that the fingerprint detector always selects the best detection statistics with the largest mean during collusion. Thus, we can model the dynamics between the colluders and the fingerprint detector as a minmax problem, where the colluders seek the minimum risk under the optimal detector and the fairness constraint, and the detector always has the maximum detection performance:

$$\min_{\{\alpha_k,\beta_l\}} \max_{\breve{F}^{(i)}} P_s^{(i)}\left(\breve{F}^{(i)}, \{\alpha_k, \beta_l\}\right) \quad (2)$$

$$\text{s.t.} \max_{\breve{F}^{(i_1)}} P_s^{(i_1)}\left(\breve{F}^{(i_1)}, \{\alpha_k, \beta_l\}\right) = \max_{\breve{F}^{(i_2)}} P_s^{(i_2)}\left(\breve{F}^{(i_2)}, \{\alpha_k, \beta_l\}\right)$$

for all $i_1, i_2 \in SC$. In (2), $\breve{F}^{(i)} = \{F_b \cup F_{e1} \cup F_{e2}, F_b, F_{e1}, F_{e2}\}$ for $i \in SC^{all}$; $\breve{F}^{(i)} = \{F_b \cup F_{e1}, F_b, F_{e1}\}$ for $i \in SC^{b,e1}$; and $\breve{F}^{(i)} = F_b$ for $i \in SC^b$.

From the analysis in [8], $P_s^{(i)}$ is determined by the mean of the detection statistics that are used. The larger the mean, the larger the

value of $P_s^{(i)}$. Therefore, for colluder $i_1 \in SC^b$, $i_2 \in SC^{b,e1}$ and $i_3 \in SC^{all}$, (2) can be simplified to

$$\begin{aligned} &\min_{\{\alpha_k,\beta_l\}} \mu = \mu_{max}^{(i_1)} = \mu_{max}^{(i_2)} = \mu_{max}^{(i_1)}, \\ \text{s.t.} \quad & 0 \le \alpha_k \le 1,\ 0 \le \beta_l \le 1, \\ \text{where} \quad & \mu_{max}^{(i_1)} = \mu_c^{(i_1)},\ \mu_{max}^{(i_2)} = \max\{\mu_b^{(i_2)}, \mu_{e1}^{(i_2)}, \mu_c^{(i_2)}\}, \\ \text{and} \quad & \mu_{max}^{(i_3)} = \max\{\mu_b^{(i_3)}, \mu_{e1}^{(i_3)}, \mu_{e2}^{(i_3)}, \mu_c^{(i_3)}\}. \end{aligned} \tag{3}$$

In (3), for user $i \in \mathbf{U}^{all}$, $\mu_c^{(i)} = E[TN^{(i)}(F_b \cup F_{e1} \cup F_{e2})]$, $\mu_b^{(i)} = E[TN^{(i)}(F_b)]$, $\mu_{e1}^{(i)} = E[TN^{(i)}(F_{e1})]$ and $\mu_{e2}^{(i)} = E[TN^{(i)}(F_{e2})]$. Similarly, for $i \in \mathbf{U}^{b,e1}$, $\mu_c^{(i)} = E[TN^{(i)}(F_b \cup F_{e1})]$, $\mu_b^{(i)} = E[TN^{(i)}(F_b)]$ and $\mu_{e1}^{(i)} = E[TN^{(i)}(F_{e1})]$. From [8],

$$\begin{aligned} &\mu_c^{(i_1)} = \frac{\beta_1\sqrt{N_b}}{K^b}\sigma_W,\ \mu_b^{(i_2)} = \frac{\beta_2\sqrt{N_b}}{K^{b,e1}}\sigma_W,\ \mu_{e1}^{(i_2)} = \frac{\alpha_1\sqrt{N_{e1}}}{K^{b,e1}}\sigma_W, \\ &\mu_c^{(i_2)} = \frac{\beta_2 N_b + \alpha_1 N_{e1}}{K^{b,e1}\sqrt{N_b+N_{e1}}}\sigma_W,\ \mu_b^{(i_3)} = \frac{(1-\beta_1-\beta_2)\sqrt{N_b}}{K^{all}}\sigma_W, \\ &\mu_{e1}^{(i_3)} = \frac{(1-\alpha_1)\sqrt{N_{e1}}}{K^{all}}\sigma_W,\ \mu_{e2}^{(i_3)} = \frac{\sqrt{N_{e2}}}{K^{all}}\sigma_W, \text{ and} \\ &\mu_c^{(i_3)} = \frac{(1-\beta_1-\beta_2)N_b + (1-\alpha_1)N_{e1} + N_{e2}}{K^{all}\sqrt{N_b+N_{e1}+N_{e2}}}\sigma_W. \end{aligned} \tag{4}$$

4. MIN-MAX SOLUTION

In this section, we'll introduce how to find the solution to the game under the constraint that all the colluders share the same risk. Given $(K^b, K^{b,e1}, K^{all})$ and (N_b, N_{e1}, N_{e2}), to search for the min-max solution, we need to first analyze $\mu_{max}^{(i)}$ for each colluder i, then find all possible collusion parameters that achieve fairness of collusion. Then, to minimize their risk, the colluders select from the feasible set the parameters that give them the minimum risk, and the fingerprint detector uses the detection statistics with the largest mean.

4.1. Analysis of $\mu_{max}^{(i)}$

For colluder $i \in SC^{b,e1}$ who receives a medium resolution copy, $\mu_{max}^{(i)}$ can be either $\mu_b^{(i)}$, $\mu_{e1}^{(i)}$ or $\mu_c^{(i)}$. If $\mu_{max}^{(i)} = \mu_b^{(i)}$, then $\mu_b^{(i)} \ge \mu_{e1}^{(i)}$ and $\mu_b^{(i)} \ge \mu_c^{(i)}$. We can show that

$$\begin{aligned} \mu_b^{(i)} \ge \mu_{e1}^{(i)} \quad &\Leftrightarrow \quad \beta_2 \ge \frac{\alpha_1\sqrt{N_{e1}}}{\sqrt{N_b}}, \text{ and} \\ \mu_b^{(i)} \ge \mu_c^{(i)} \quad &\Leftrightarrow \quad \beta_2 \ge \frac{\alpha_1 N_{e1}}{\sqrt{N_b}(\sqrt{N_b+N_{e1}}-\sqrt{N_b})}. \end{aligned} \tag{5}$$

Since $\sqrt{N_{e1}} \ge \sqrt{N_b+N_{e1}} - \sqrt{N_b}$, so (5) can be simplified to

$$\mu_{max}^{(i)} = \mu_b^{(i)} \text{ if and only if } \beta_2 \ge \frac{\alpha_1 N_{e1}}{\sqrt{N_b}(\sqrt{N_b+N_{e1}}-\sqrt{N_b})}. \tag{6}$$

The analysis for $\mu_{max}^{(i)} = \mu_{e1}^{(i)}$ and $\mu_{max}^{(i)} = \mu_c^{(i)}$ are similar and detailed derivation is in [10].

For colluder $i \in SC^{all}$ who receive all three layers, $\mu_{max}^{(i)}$ has four possible values: $\mathbf{u}_{max}^{(i)} = \mathbf{u}_b^{(i)}$, $\mathbf{u}_{max}^{(i)} = \mathbf{u}_{e1}^{(i)}$, $\mathbf{u}_{max}^{(i)} = \mathbf{u}_{e2}^{(i)}$, and $\mathbf{u}_{max}^{(i)} = \mathbf{u}_c^{(i)}$. The analysis is similar to (5), and detailed derivation is in [10]. From [10], if $N_{e2} > N_b$, $\mu_b^{(i)}$ cannot the largest among the four means, and $\mu_{max}^{(i)} \ne \mu_{e1}^{(i)}$ if $N_{e1} > N_b$.

4.2. Feasible Set

Given the above analysis, the next step for colluders is to find all possible sets of $\{\alpha_k, \beta_l\}$ that satisfy $\mu_{max}^{(i_1)} = \mu_{max}^{(i_2)} = \mu_{max}^{(i_3)}$ for $i_1 \in SC^b$, $i_2 \in SC^{b,e1}$ and $i_3 \in SC^{all}$.

Without loss of generality, we consider a scalable fingerprinting system where $N_b : N_{e1} : N_{e2} = 1 : 1 : 2$. In this scenario, from the analysis in the previous section, for a colluder $i_2 \in SC^{b,e1}$ who receives a medium resolution copy, $\mu_{max}^{(i_2)}$ has three possible values: $\mu_{max}^{(i_2)} = \mu_b^{(i_2)}$, $\mu_{max}^{(i_2)} = \mu_{e1}^{(i_2)}$ and $\mu_{max}^{(i_2)} = \mu_c^{(i_2)}$. Furthermore, for a colluder $i_3 \in SC^{all}$ who receives all three layers, $\mu_{max}^{(i_3)}$ equals to either $\mu_{e1}^{(i_3)}$ or $\mu_c^{(i_3)}$, while $\mu_{max}^{(i_3)} \ne \mu_b^{(i_3)}$ and $\mu_{max}^{(i_3)} \ne \mu_{e1}^{(i_3)}$. Thus, there are a total of 6 possible combinations of $\mu_{max}^{(i_2)}$ and $\mu_{max}^{(i_3)}$.

The first one is $\mu_{max}^{(i_2)} = \mu_b^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{max}^{(i_3)} = \mu_{e2}^{(i_3)}$ for $i_3 \in SC^{all}$. From (4), $\mu_{max}^{(i_1)} = \beta_1\sqrt{N_b}\sigma_W/K^b$, $\mu_{max}^{(i_2)} = \beta_2\sqrt{N_b}\sigma_W/K^{b,e1}$, and $\mu_{max}^{(i_3)} = \sqrt{N_{e2}}\sigma_W K^{all}$. To let $\mu_{max}^{(i_1)} = \mu_{max}^{(i_2)} = \mu_{max}^{(i_3)}$, colluders should select

$$\beta_1 = \frac{\sqrt{N_{e2}}K^b}{\sqrt{N_b}K^{all}} = \frac{\sqrt{2}K^b}{K^{all}} \text{ and } \beta_2 = \frac{\sqrt{2}K^{b,e1}}{K^{all}}. \tag{7}$$

Because the selected β_1 and β_2 have the constraint $0 \le \beta_1, \beta_2 \le \beta_1 + \beta_2 \le 1$, therefore, $(K^b, K^{b,e1}, K^{all})$ must satisfy

$$\beta_1 + \beta_2 = \sqrt{2}\frac{K^b + K^{b,e1}}{K^{all}} \le 1 \quad \Leftrightarrow \quad K^{all} \ge \frac{\sqrt{2}K}{1+\sqrt{2}}. \tag{8}$$

From (6), $\mu_{max}^{(i_2)} = \mu_b^{(i_2)}$ if and only if

$$\begin{aligned} \alpha_1 \le A \quad &\triangleq \quad \beta_2\frac{\sqrt{N_b}(\sqrt{N_b+N_{e1}}-\sqrt{N_b})}{N_{e1}} \\ &= \quad \frac{\sqrt{2N_b}(\sqrt{N_b+N_{e1}}-\sqrt{N_b})}{N_{e1}}\frac{K^{b,e1}}{K^{all}}. \end{aligned} \tag{9}$$

$A = (2-\sqrt{2})K^{b,e1}/K^{all}$ in our example of $N_b : N_{e1} : N_{e2} = 1 : 1 : 2$. Similarly, $\mu_{max}^{(i_3)} = \mu_{e2}^{(i_3)}$ if and only if

$$\begin{aligned} \alpha_1 \ge B \quad &\triangleq \quad 1 + \frac{(1-\beta_1-\beta_2)N_b + N_{e2}}{N_{e1}} \\ &\quad -\frac{\sqrt{N_{e2}}\cdot\sqrt{N_b+N_{e1}+N_{e2}}}{N_{e1}} \end{aligned} \tag{10}$$

$B = 4-2\sqrt{2}-\sqrt{2}(K^b+K^{b,e1})/K^{all}$ if $N_b : N_{e1} : N_{e2} = 1 : 1 : 2$. In order to be able to select a α_1 that satisfies both $B \le \alpha_1 \le A$ and $0 \le \alpha_1 \le 1$, it is required that $A \ge 0$ (which is always true for all $K^{b,e1} \ge 0$ and $K^{all} \ge 0$) , $B \le 1$ and $B \le A$. Consequently, $(K^b, K^{b,e1}, K^{all})$ must satisfy

$$\begin{aligned} B \le 1 \quad &\Leftrightarrow \quad K^{all} \le \frac{\sqrt{2}K}{3-\sqrt{2}}, \\ \text{and } B \le A \quad &\Leftrightarrow \quad K^{all} \le \frac{2K-(2-\sqrt{2})K^b}{6-2\sqrt{2}}. \end{aligned} \tag{11}$$

Combining (8) and (11), we have

$$\frac{\sqrt{2}K}{1+\sqrt{2}} \le K^{all} \le \min\left\{\frac{2K-(2-\sqrt{2})K^b}{6-2\sqrt{2}}, K-K^b\right\}. \tag{12}$$

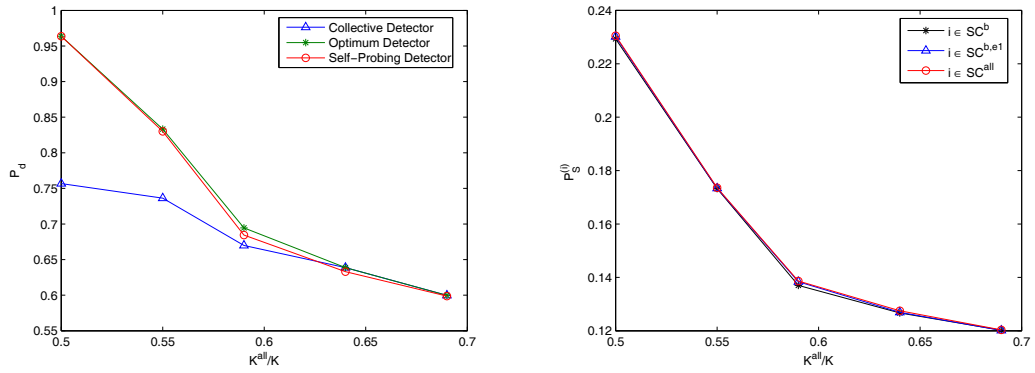
To summarize, if $(K^b, K^{b,e1}, K^{all})$ satisfies (12), colluders can ensure the equal risk by following (7)-(10) when selecting the collusion parameters. In this scenario, $\mu_{max}^{(i_2)} = \mu_b^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{max}^{(i_3)} = \mu_{e2}^{(i_3)}$ for $i \in SC^{all}$. The analysis for other combinations of $\mu_{max}^{(i_2)}$ and $\mu_{max}^{(i_3)}$ are similar, and the details are in [10].

4.3. Min-Max Solution

After identify all the possible collusion parameters that satisfy $\mu_{max}^{(i_1)} = \mu_{max}^{b,e1} = \mu_{max}^{all}$, to find the solution of this colluder-detector game, colluders should find collusion parameters in the feasible set that gives them the smallest risk, and the fingerprint detector should use the detection statistics with the largest mean.

To demonstrate this process, we use the system setup in Figure 1 as an example, where $N_b = 5000$, $N_{e1} = 5000$ and $N_{e2} = 10000$, respectively. Among a total of $K = 250$ colluders, if $K^b = 50$, $K^{b,e1} = 25$, and $K^{all} = 175$, for $i_2 \in SC^{b,e1}$ and $i_3 \in SC^{all}$, there are three scenarios where colluder can have equal risk:

• The colluders can achieve fairness of collusion by selecting $\beta_1 = 0.4594$, $0.0951 \le \alpha_1 \le 0.2297$ and $\beta_2 = 0.3248 - \alpha_1$. In this scenario, $\mu_{max}^{(i_2)} = \mu_c^{(i_2)} = \mu_{max}^{(i_3)} = \mu_c^{(i_3)} = 2.0545$.



(a) (b)

Fig. 2. Simulation results on the first 40 frames of sequence "carphone" from 10000 simulation runs. (a): P_d of the collective fingerprint detector, the optimum detector and the self-probing detector. (b) Each colluder's probability of being detected ($P_s^{(i)}$) with the self-probing detector. $(N_b, N_{e1}, N_{e2}) = (42987, 42951, 85670)$. $|\mathbf{U}^b| = |\mathbf{U}^{b,e1}| = |\mathbf{U}^{all}| = 250$. $P_{fp} = 10^{-3}$. $K = 250$ and $K^b = 50$. Each point on the x axis corresponds to a unique triplet $(K^b, K^{b,e1}, K^{all})$ where $K^{b,e1} = K - K^b - K^{all}$. $P_{fp} = 10^{-3}$.

• The second scenario is when colluders select $0.4594 \leq \beta_1 \leq 1$, $\beta_2 = \frac{K^{b,e1}}{K^b}\beta_1$ and $\alpha_1 = 4 - \frac{K+K^{all}}{K^b}\beta_1$. Here, $\mu_{max}^{(i_2)} = \mu_b^{(i_2)} = \mu_{max}^{(i_3)} = \mu_c^{(i_3)}$. Among all these feasible sets of collusion parameters, $\mu_{max}^{(i)}$ is minimized when $\beta_1 = 0.4594$, $\beta_2 = 0.2297$ and $\alpha_1 = 0.0951$, and $\mu_{max}^{(i_2)} = \mu_b^{(i_2)} = \mu_c^{(i_2)} = 2.0545$.

• In the third scenario, $0.4594 \leq \beta_1 \leq 1$, $\beta_2 = 4 - \frac{K+K^{all}}{K^b}\beta_1$ and $\alpha_1 = \frac{K^{b,e1}}{K^b}\beta_1$, which gives $\mu_{max}^{(i_2)} = \mu_{e1}^{(i_2)} = \mu_{max}^{(i_3)} = \mu_c^{(i_3)}$. $\mu_{max}^{(i)}$ is minimized and equals to 2.0545 when $\beta_1 = 0.4594$, $\beta_2 = 0.0951$ and $\alpha_1 = 0.2297$, which gives $\mu_{max}^{(i_2)} = \mu_{e1}^{(i_2)} = \mu_c^{(i_2)}$.

Therefore, the solution for this example is: colluders uses $\beta_1 = 0.4594$, $0.0951 \leq \alpha_1 \leq 0.2297$ and $\beta_2 = 0.3248 - \alpha_1$, and the fingerprint detector uses fingerprints extracted from all layers collectively to identify colluders. By the above analysis, colluders can't further reduce their risk while still achieving fairness, and the fingerprint detector can't further improve the traitor tracing performance neither. Thus, this solution is optimal for all the players in the game.

5. SIMULATION RESULTS

We test on the first 40 frames of sequence "carphone" and choose $F_b = \{1, 5, 9, \cdots, \}$, $F_{e1} = \{3, 7, 11, \cdots\}$ and $F_{e2} = \{2, 4, 6, \cdots\}$ as an example of temporal scalability. We use human visual model based spread spectrum embedding [7] when embedding fingerprints into the host signal, and assign orthogonal fingerprints to different users. During collusion, colluders apply two-stage collusion in Section 2.2 and follow Section 4 when selecting collusion parameters. For each frame in the colluded copy, we adjust the power of the additive noise such that $||\mathbf{n}_j||^2 = ||\mathbf{W}_j^{(i)}||^2$.

We simulate three different types of fingerprint detectors: the simple collective detector in [5] which always uses fingerprints extracted from all layers to identify colluders; a optimum detector which has perfect knowledge of the means of the detection statistics and always selects the one with the best detection performance; and the self-probing detector in [8] which first probes information about the means of the detection statistics and then selects the detection statistics with the largest estimated mean.

Figure 2 (a) shows the performance of different detectors. From Figure 2 (a), using side information about the means of the detection statistics during fingerprint detection help improve the traitor tracing performance, and the performance of the self-probing fingerprint detector is approximately the same as that of the optimum detector. Figure 2 (b) plots each colluder's probability of being detected with the self-probing fingerprint detector. By choosing the collusion parameters as in Section 4, all colluders have the same probability of being detected and achieve fairness of collusion.

6. CONCLUSIONS

This paper investigates the game-theoretic formulation and analysis of the dynamics between the colluders and the fingerprint detector. We model this dynamics as a two-stage zero-sum game, where the colluders select the collusion parameters to minimize their risk under the fairness constraint, and the fingerprint detector probes side information about collusion and adaptively adjust the detection strategy to maximize the collusion resistance. We analyze the existence of the optimal solution where no players in the game can further increase their payoff, and derive the strategy for the colluders and the fingerprint detector to reach if it exists.

7. REFERENCES

[1] F. Zane, "Efficient watermark detection and collusion security," *Proc. of 4th International Conf. on Financial Cryptography, Lecture Notes in Computer Science*, vol. 1962, pp. 21–32, Feb. 2000.

[2] J. Dittmann, P. Schmitt, E. Saar, J. Schwenk, and J. Ueberberg, "Combining digital watermarks and collusion secure fingerprints for digital images," *SPIE Journal of Electronic Imaging*, vol. 9, no. 4, pp. 456–467, Oct. 2000.

[3] W. Trappe, M. Wu, Z. Wang, and K. J. R. Liu, "Anti-collusion fingerprinting for multimedia," *IEEE Tran. on Signal Processing*, vol. 51, no. 4, pp. 1069–1087, April 2003.

[4] Y. Wang, J. Ostermann, and Y. Zhang, *Video Processing and Communications*, Prentice Hall, 1st edition, 2001.

[5] H. V. Zhao and K. J. R. Liu, "Behavior forensics for scalable multiuser collusion: Fairness and effectiveness," *IEEE Tran. on Information Forensics and Security*, vol. 1, no. 3, pp. 311–329, Sept. 2006.

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

[7] 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.

[8] W. S. Lin, H. V. Zhao, and K. J. R. Liu, "Scalable multimedia fingerprinting forensics with side information," *IEEE Int. Conf. on Image Processing*, Oct. 2006.

[9] D. Fudenberg and J. Tirole, *Game Theory*, The MIT Press, 1991.

[10] W. S. Lin, H. V. Zhao, and K. J. R. Liu, "Colluder-detector behavior forensics: Game-theoretic formulation and analysis," *submitted to IEEE Transcations on Information Forensics and Security*.