# Behavior Forensics With Side Information for Multimedia Fingerprinting Social Networks

W. Sabrina Lin, H. Vicky Zhao, and K. J. Ray Liu, *Fellow, IEEE*

***Abstract*—In multimedia social networks, there exists complicated dynamics among users who share and exchange multimedia content. Using multimedia fingerprinting as an example, this paper investigates the human behavior dynamics in the multimedia social networks with side information. Side information is the information other than the colluded multimedia content that can help increase the probability of detection. We study the impact of side information in multimedia fingerprinting and show that the statistical means of the detection statistics can help the fingerprint detector significantly improve the collusion resistance. We then investigate how to probe the side information and model the dynamics between the fingerprint detector and the colluders as a two-stage extensive game with perfect information. We model the colluder-detector behavior dynamics as a two-stage game and find the equilibrium of the colluder-detector game using backward induction and show that the min-max solution is a Nash equilibrium, which gives no incentive for everyone in the multimedia fingerprint social network to deviate. This paper demonstrates that the proposed side information can significantly help improve the system performance to almost the same as the optimal correlation-based detector. Such result opens up a new scope in the research of fingerprinting system that given any fingerprint code, leveraging side information can improve the collusion resistance. Also, we provide the solutions to how to reach optimal collusion strategy and the corresponding detection, thus lead to a better protection of the multimedia content.**

***Index Terms*—Behavior forensics, collusion attack, multimedia fingerprinting, side information, social networks.**

## I. Introduction

A SOCIAL network is a structure of nodes, which are usually individuals or organizations, that are connected with each other via certain types of relations, such as values, friendship, conflict, financial exchange, trade, etc. A *multimedia social network* is a social network in which a group of users share and exchange multimedia content, as well as other resources, e.g., Napster, Youtube, etc. By participating in multimedia social networks, users exchange resources with others. Since these multimedia social networks include millions of people, a crucial issue there is to understand the user dynamics that influence human behavior [1], such as how users interact with and respond to each other. Research on human behavior provides fundamental guidelines to better design of multimedia systems and to offer more reliable and personalized services. For example, the performance of a peer-to-peer system fully depends on how cooperative the users are. If the designer of a peer-to-peer system can analyze the user behavior, he/she can predict the performance and design mechanisms to construct a better system.

In this paper, we illustrate how to model and analyze user dynamics in multimedia social networks using multimedia fingerprinting as an example. Multimedia fingerprinting is an emerging forensic tool to protect multimedia from illegal alteration and unauthorized redistribution. It uses traditional data-hiding techniques [2] to embed a unique label, known as "fingerprint," into each distributed copy to track the usage of multimedia data. Multiuser collusion is a powerful attack against multimedia fingerprinting, where a group of attackers collectively and effectively mount attacks to remove traces of the identifying fingerprints [3]. To offer consistent and reliable traitor tracing, multimedia fingerprinting should resist such multiuser collusion as well as attacks by a single adversary [4].

In the literature, there has been a lot of prior work on the modelling and analysis of collusion [5]–[7]. The work in [8] studied the relationship between the maximum allowable colluders by a fingerprinting system and other parameters, e.g., the fingerprint length, the total number of users, and the system requirements. Linear and nonlinear collusion attacks on orthogonal fingerprints were studied in [9], and the work in [10] investigated how a selfish colluder behave if he/she wants to cheat during multiuser collusion in order to further decrease his/her risk. Based on the above investigations, techniques from different disciplines, including error-correcting codes, finite-projective geometry, and combinatorial theories, have been used in the literature to design multimedia fingerprints that can resist collusion attacks [11]–[14].

In multimedia fingerprinting, colluders and the fingerprint detector form a multimedia social network: colluders who apply multiuser collusion attempt to remove the identifying fingerprints in their copies, and the digital rights enforcer detects the embedded fingerprints in the suspicious copy to capture colluders. It is obvious that the colluders and the fingerprint detector influence each other's performance and decision: given a colluded copy, the detector always wants to adjust his/her detection strategy to achieve the best possible traitor-tracing performance. Meanwhile, during collusion, the colluders try the best to minimize their risk based on the available information

Manuscript received October 30, 2008; revised August 14, 2009. First published September 29, 2009; current version published November 18, 2009. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. M. Kivanc Mihcak.

W. S. Lin and K. J. R. Liu are with the Department of Electrical and Computer Engineering, Institute for Systems Research, University of Maryland, College Park, MD 20742 USA (e-mail: wylin@eng.umd.edu; kjrliu@eng.umd.edu).

H. V. Zhaoy is with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, Alberta T6G 2V4, Canada (e-mail: vzhao@ece.ualberta.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2009.2033224

about the detection procedure. There are many collusion strategies that the colluders can use to remove the identifying fingerprints. Also, the detector can apply different detection strategies to identify the colluders. Thus, the dynamics between the colluders and the fingerprint detector is complicated.

In this paper, we investigate two important issues in multimedia fingerprinting social networks. First, we study the impact of the dynamics between the two group of users (colluders and the fingerprint detector) in the social network when *side information* is available. Second, we model the user dynamics using a game-theoretic framework and find the optimal strategies for all users.

In multimedia fingerprinting, colluders and the fingerprint detector influence each other's decision and performance. To maximize their own payoff, each player should observe and learn how others play the game and adjust his/her strategy accordingly. The previous work [15] on behavior forensics assumed that the fingerprint detector has no information about multiuser collusion. If some information of collusion attacks can be made available during the colluder identification process, intuitively, utilizing such information can help improve the traitor tracing performance. We define this information about collusion that can improve detection probability as side information. We consider the worst case for the fingerprint detector that all he/she has for detection is the colluded copy. Unlike side channels in digital communication, side information about collusion in multimedia fingerprinting systems can only be extracted from the colluded copy. In this paper, we explore techniques that enable the detector to probe and utilize side information and analyze its performance. We find that the mean value of the detection statistics of each user is a very useful side information and can significantly improved the detection performance. Then by formulating the colluder-detector behavior with a game theoretical framework, we further study the dynamics from the opposite point of view, analyzing how colluders should adjust the collusion attacks to minimize their probability of being detected. Once the detector improves the traitor tracing performance by utilizing side information, the colluders might also change their collusion strategy to minimize their risk. Thus, the optimal strategy of the users in the multimedia fingerprinting social network will be changed and the user dynamics will also reach a new equilibrium.

The rest of the paper is organized as follows. Section II introduces the multimedia fingerprinting system. In Section III, we investigate how the fingerprint detector probes and utilizes side information about collusion to improve the collusion resistance. In Section IV, we analyze the equilibrium of the colluder-detector game, study the colluders' strategies to minimize their risk under the fairness constraint, and finds the solution to the min-max formulation of the colluder-detector dynamics. Section V shows the simulation results, and conclusions are drawn in Section VI.

## II. Multimedia Fingerprinting System

In this section, we will review the structure and users involved in a multimedia fingerprinting social network.

### A. Temporally Scalable Video Coding Systems

As multimedia networking develops, scalability in multimedia coding becomes increasingly important for rich media access from anywhere by anyone [16]. Scalable video coding 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.

Without loss of generality, we use temporally scalable video coding as an example which provides multiple versions of the same video with different frame rates. Following the same model in [15], we consider a temporally scalable video coding system with three-layer scalability, and we use frame skipping and frame copying to implement temporal decimation and interpolation, respectively. In such a video coding system, different frames in the video sequence are encoded in different layers. Define $F_b$, $F_{e1}$, and $F_{e2}$ as the sets containing indexes of the frames that are encoded in the base layer, enhancement layer 1 and enhancement layer 2, respectively. $F^{(i)}$ includes the indexes of the frames in the copy that user $\mathbf{u}^{(i)}$ receives. $\mathbf{U}^b = \{i : F^{(i)} = F_b\}$ is the subgroup of users who receive the base layer only, $\mathbf{U}^{b,e1} = \{i : F^{(i)} = F_b \cup F_{e1}\}$ contains all users who subscribe to the medium-resolution version with the base layer and the enhancement layer 1, and $\mathbf{U}^{\text{all}} = \{i : F^{(i)} = F_b \cup F_{e1} \cup F_{e2}\}$ contains the indexes of the users who receive all three layers.

### B. Multimedia Fingerprinting System and Collusion Attacks

*1) Fingerprint Embedding:* Proven to be robust against many single-copy attacks and common signal processing, spread spectrum embedding is a popular data hiding technique to embed fingerprints into the host multimedia signals [3], [17]. For the $j^{\text{th}}$ frame in the video sequence represented by a vector $\mathbf{S}_j$, and for each user $\mathbf{u}^{(i)}$ who subscribes to frame $j$, the content owner generates a unique fingerprint $\mathbf{W}_j^{(i)}$ of the same length as $\mathbf{S}_j$. The fingerprinted frame j that is distributed to $\mathbf{u}^{(i)}$ is $X_j^{(i)}(k) = S_j(k) + JND_j(k) \cdot W_j^{(i)}(k)$, where $X_j^{(i)}(k)$, $S_j(k)$ and $W_j^{(i)}(k)$ are the $k$th components of the fingerprinted frame $\mathbf{X}_j^{(i)}$, the host signal $\mathbf{S}_j$ and the fingerprint vector $\mathbf{W}_j^{(i)}$, respectively. $JND_j$ is used to control the energy and achieve the imperceptibility of the embedded fingerprints [17].

We consider orthogonal fingerprint modulation [5] in this paper. We first generate independent vectors following Gaussian distribution $\mathcal{N}(0, \sigma_W^2)$, and then apply Gram-Schmidt orthogonalization to produce fingerprints that are strictly orthogonal to each other with equal energies.

*2) Collusion Attacks:* During multiuser collusion, attackers collectively mount attacks to effectively remove traces of the embedded fingerprints. Since no one is willing to take a higher risk than the others, an important issue during collusion is to distribute the risk evenly among colluders and achieve fairness of the attack. As studied in [9], given the same amount of noise,

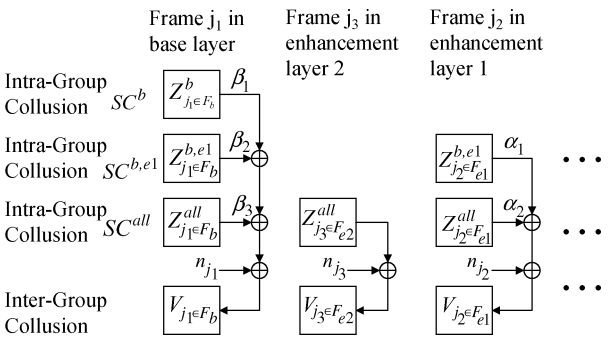



Fig. 1. Two-stage collusion for scalable-encoded multimedia content.

for Gaussian fingerprint, the nonlinear attack can be modelled as averaging attack. The work in [15] studied how to ensure that all attackers have the same probability of being captured when they receive fingerprinted copies of different quality due to network and device heterogeneity.

Let $SC^b$ be the set with the indexes of the colluders who receive the fingerprinted base layer only; $SC^{b,e1}$ contains the indexes of all colluders who subscribe to the medium resolution copy; and $SC^{\text{all}}$ contains the indexes of the colluders who receive all three layers. $K^b = |SC^b|$, $K^{b,e1} = |SC^{b,e1}|$, and $K^{\text{all}} = |SC^{\text{all}}|$ are the number of colluders in $SC^b$, $SC^{b,e1}$ and $SC^{\text{all}}$, respectively. $K = K^b + K^{b,e1} + K^{\text{all}}$ is the total number of colluders.

Following the two-stage collusion model in [15], colluders first apply intragroup collusion as shown in Fig. 1. For each frame $j \in F_b$ in the base layer, colluders in $SC^b$ 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 $j = F_b \cup F_{e1} \cup F_{e2}$ in the video sequence, the colluders in $SC^{\text{all}}$ generate $\mathbf{Z}_j^{\text{all}} = \sum_{k \in SC^{\text{all}}} \mathbf{X}_j^{(k)}/K^{\text{all}}$. Then, colluders combine these three copies, $\{\mathbf{Z}_j^b\}_{j \in F_b}$, $\{\mathbf{Z}_j^{b,e1}\}_{j \in F_b \cup F_{e1}}$, and $\{\mathbf{Z}_j^{\text{all}}\}_{j \in F_b \cup F_{e1} \cup F_{e2}}$, and apply intergroup collusion. For each frame $j \in F_b$ in the base layer, the colluded frame is

$$\mathbf{V}_j = \beta_1 \mathbf{Z}_j^b + \beta_2 \mathbf{Z}_j^{b,e1} + (1 - \beta_1 - \beta_2)\mathbf{Z}_j^{\text{all}} + \mathbf{n}_j \quad (1)$$

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, colluders calculate

$$\mathbf{V}_{j_2} = \alpha_1 \mathbf{Z}_{j_2}^{b,e1} + (1 - \alpha_1)\mathbf{Z}_{j_2}^{\text{all}} + \mathbf{n}_{j_2} \quad (2)$$

where $0 \le \alpha_1 \le 1$. For each frame $j_3 \in F_{e2}$ in the enhancement layer 2, the colluded frame $j$ is

$$\mathbf{V}_{j_3} = \mathbf{Z}_{j_3}^{\text{all}} + \mathbf{n}_{j_3}. \quad (3)$$

$\mathbf{n}_j$ is additive noise to further hinder detection.

During collusion, the colluders seek the collusion parameters $\alpha_1, \beta_1$, and $\beta_2$ to minimize their risk under the constraint that all colluders have the same probability of being detected. From the above collusion model, the collusion parameters $\alpha_j, \beta_l$ directly reflect the collusion strategy. And the side information we will discuss in the following sections is the information hidden in the colluded copy that can give detector better estimation of the collusion, and lead to a better detection performance. If the detector iscorrelation-based, then the mean value of the detection statistics can be used as side information, which we will show in Section III.

*3) Fingerprint Detection and Colluder Identification:* We consider a nonblind detection scenario where the host signal is first removed from the test copy before colluder identification. The detector then extracts the fingerprint $\mathbf{Y}_j$ from the $j^{th}$ frame $\mathbf{V}_j$ in the colluded copy. Then, he/she calculates the similarity between the extracted fingerprint $\mathbf{Y}$ and each of the original fingerprints $\{\mathbf{W}^{(i)}\}$, compares with a predetermined threshold $h$, and outputs the estimated identities of the colluders $\widehat{SC}$.

To analyze the performance of multimedia fingerprints, we adopt the commonly used criteria in the literature [5]. In order to measure the performance of the fingerprint system under various conditions, such as top-secret scenario in which the fingerprint detector aim to catch as many colluders as possible and the popular commercial scenario in which the non of the innocent user should be falsely accused. Let $P_d^{(i)}$ is the probability of user $i$ being accused as a colluder, we use the following measurements:

- $P_d$: the probability of capturing at least one colluder. The motivating application of $P_d$ is to provide digital evidence in the court of law. When a user is identified as a colluder and $P_d$ is high, the content owner can confidentially accuse the user being guilty. From the analysis in [5], $P_d$ can be formulated as $1 - \prod_{i \in SC}(1 - P_d^{(i)})$, where $SC$ is the set of the colluders.
- $P_{fp}$: the probability of accusing at least one innocent user. $P_{fa}$ serves as the probability of false alarm in high-security system. It reflects the confidence of the detector about the accused users—the lower the $P_{fa}$ is, the higher the detection confidence. $P_{fa}$ can be formulated as $1 - \prod_{i \notin SC}(1 - P_d^{(i)})$.
- $E[F_d]$: the expected fraction of colluders that are successfully captured. When the digital rights enforcer's concern is to catch as many colluders as possible, $E[F_d]$ is a suitable performance criteria. Mathematically, $E[F_d] = \sum_{i \in SC} P_d^{(i)}/K$, where K is the number of colluders.
- $E[F_{fp}]$: the expected fraction of innocent users that are falsely accused. $E[F_{fp}]$ and $E[F_d]$ are used to show the balance between capturing colluders and placing innocents under suspicion, where $E[F_{fp}] = \sum_{i \notin SC} P_d^{(i)}/(M - K)$. Here, $M$ is the total number of users.

## III. Analysis of Detector's Strategies With Side Information

This section analyzes how side information about collusion can help improve the collusion resistance and influence the detector's action. We study how to probe side information about collusion from the colluded copy. Consider the scenario where the colluded copy contains all three layers and has the highest quality, and the analysis for other scenarios, such if the colluders only have two layers of the video, is similar. Without loss of generality, we use users in $\mathbf{U}^{\text{all}}$ as an example to demonstrate

the detection process and analyze the performance. For users in $\mathbf{U}^{b,e1}$ and $\mathbf{U}^{b}$, the colluder identification process and the performance analysis are similar.

### A. Different Fingerprint Detection Strategies

As we discussed in Section II-B-3, when detecting fingerprints, there are many different ways to measure the similarity between the extracted fingerprint $\mathbf{Y}$ and the originally embedded one $\mathbf{W}^{(i)}$.

*1) A Collective Fingerprint Detector:* The work in [15] considered a simple fingerprint detector that uses fingerprints extracted from all layers collectively to identify colluders. For each user $\mathbf{u}^{(i)}$, the detector first calculates $\breve{F}^{(i)} = F^{(i)} \cap F^{c}$, where $F^{(i)}$ contains the indexes of the frames received by $\mathbf{u}^{(i)}$ and $F^{c}$ contains the indexes of the frames in the colluded copy. Then, the detector calculates

$$TN_c^{(i)} = \left( \sum_{j \in \breve{F}^{(i)}} \left\langle \mathbf{Y}_j, \mathbf{W}_j^{(i)} \right\rangle \right) / \sqrt{\sum_{j \in \breve{F}^{(i)}} \left\| \mathbf{W}_j^{(i)} \right\|^2} \quad (4)$$

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

Assume that the colluders choose the parameters $\{\alpha_k, \beta_l\}$ in the same way as in [15]. Without loss of generality, we consider the scenario where the colluders generate a colluded copy of the highest resolution and $F^c = F_b \cup F_{e1} \cup F_{e2}$ [18]. With orthogonal fingerprint modulation as in Section II-B-1, under the assumption that the detection noises are i.i.d. and follow Gaussian distribution $\mathcal{N}(0, \sigma_n^2)$, the detection statistics $\{TN_c^{(i)}\}$ in (4) are independent Gaussian with marginal distribution

$$TN_c^{(i)} \sim \begin{cases} \mathcal{N}\left(\mu_c^{(i)}, \sigma_n^2\right), & \text{if } i \in SC \\ \mathcal{N}\left(0, \sigma_n^2\right), & \text{if } i \notin SC \end{cases}$$

where

$$\mu_c^{(i)} = \frac{(1-\beta_1-\beta_2)N_b + (1-\alpha_1)N_{e1} + N_{e2}}{K^{\text{all}}\sqrt{N_b + N_{e1} + N_{e2}}} \sigma_W^2.$$

$N_b$, $N_{e1}$, and $N_{e2}$ are the lengths of the fingerprints embedded in the base layer, enhancement layer 1 and enhancement layer 2, respectively. For a given user $\mathbf{u}^{(i)}$, define $P_s^{(i)}$ as the probability of successfully capturing him/her if he/she is guilty, and $P_{fa}^{(i)}$ is the probability of falsely accusing him/her if he/she is innocent. With the detector in (4), we have

$$P_s^{(i)} = Q\left(\frac{h - \mu_c^{(i)}}{\sigma_n}\right), \quad \text{if} \quad i \in SC$$

and

$$P_{fa}^{(i)} = Q\left(\frac{h}{\sigma_n}\right), \quad \text{if} \quad i \notin SC \quad (5)$$

where $Q(\cdot)$ is the Gaussian tail function. Therefore, the four criterions for the fingerprint detector can be formulated as in (6).

$$\begin{aligned} P_d &= P\left[\max_{i \in SC} TN_c^{(i)} > h\right] = 1 - \prod_{i \in SC} P_s^{(i)} \\ &= 1 - \left[1 - Q\left(\frac{h - \mu_c^{(i)}}{\sigma_n}\right)\right]^K \\ P_{fp} &= P\left[\max_{i \notin SC} TN_c^{(i)} > h\right] = 1 - \prod_{i \notin SC} \left(1 - P_{fa}^{(i)}\right) \\ &= 1 - \left[1 - Q\left(\frac{h}{\sigma_n}\right)\right]^{M-K} \\ E[F_d] &= \sum_{i \in SC} P\left[TN_c^{(i)} > h\right]/K = \sum_{i \in SC} P_s^{(i)}/K \\ &= Q\left(\frac{h - \mu_c^{(i)}}{\sigma_n}\right) \end{aligned}$$

and

$$\begin{aligned} E[F_{fp}] &= \sum_{i \notin SC} P\left[TN_c^{(i)} > h\right]/(M-K) \\ &= \sum_{i \notin SC} P_{fa}^{(i)}/(M-K) = Q\left(\frac{h}{\sigma_n}\right). \end{aligned} \quad (6)$$

Assuming that the fingerprint detector will always use (5) and fingerprints extracted from all layers collectively to determine if $\mathbf{u}^{(i)}$ participates in collusion, the work in [15] studied how the colluders should select the parameters $\alpha_1$, $\beta_1$ and $\beta_2$ such that $\{P_s^{(i)}\}$ are the same for all colluders $i \in SC$ and will be compared with the results in Section IV.

*2) Fingerprint Detection at Each Individual Layer:* Given $\mathbf{Y}_{e2}$, $\mathbf{Y}_{e1}$ and $\mathbf{Y}_b$ which are the fingerprints extracted from the enhancement layer 2, enhancement layer 1 and the base layer, respectively, in addition to the collective detector (4) in Section III-A-1, the digital rights enforcer can also examine $\mathbf{Y}_{e2}$, $\mathbf{Y}_{e1}$ and $\mathbf{Y}_b$ independently and use the detection results at each individual layer to estimate the colluders' identities. Therefore, in addition to the collective detector, the digital rights enforcer can also use *detectors at base layer, enhancement layer1, and enhancement layer 2*. To demonstrate this colluder identification process and analyze its performance, we use users in $\mathbf{U}^{\text{all}}$ who receive all three layers as an example. The analysis for users in $\mathbf{U}^{b,e1}$ and $\mathbf{U}^{b}$ is similar and thus omitted.

Let $F_t$ be the set of indexes of the frames in layer $t$ in which $t = b, e1, e2$ represents base layer, enhancement layer 1, and enhancement layer 2, respectively. For user $\mathbf{u}^i \in \mathbf{U}^{\text{all}}$ who receive all three layers from the content owner, given $\{\mathbf{Y}_j\}_{j \in F_t}$, the fingerprints from layer $t$ of the colluded copy, the detector at layer $t$ calculates the detection statistics

$$TN_t^{(i)} = \left( \sum_{j \in F_t} \left\langle \mathbf{Y}_j, \mathbf{W}_j^{(i)} \right\rangle \right) / \sqrt{\sum_{j \in F_t} \left\| \mathbf{W}_j^{(i)} \right\|^2} \quad (7)$$

to measure the similarity between the extracted fingerprint and the originally embedded fingerprint. The detector at layer $t$ accused $u^{(i)}$ as a colluder if $TN_t^{(i)} > h$, and sets $i \in \widehat{SC}$, which is the suspicious-colluder set. Here, $h$ here is a predetermined threshold.

The analysis of the detection statistics $TN_t^{(i)}$ in (8) is similar to that of $TN^{(i)}$ in (4). If the detection noises are i.i.d. and follow Gaussian distribution $\mathcal{N}(0,\sigma_n^2)$, for user $\mathbf{u}^{(i)} \in \mathbf{U}^{\text{all}}$, $TN_t^{(i)}$ are independent Gaussian with marginal distribution

$$TN_t^{(i)} \sim \begin{cases} \mathcal{N}\left(\mu_t^{(i)}, \sigma_n^2\right), & \text{if } i \in SC \\ \mathcal{N}\left(0, \sigma_n^2\right), & \text{if } i \notin SC \end{cases}$$

where

$$\mu_b^{(i)} = (1-\beta_1-\beta_2)\frac{\sqrt{N_b}}{K^{\text{all}}}\sigma_W$$
$$\mu_{e1}^{(i)} = (1-\alpha_1)\frac{\sqrt{N_{e1}}}{K^{\text{all}}}\sigma_W \text{ and } \mu_{e2}^{(i)} = \frac{\sqrt{N_{e2}}}{K^{\text{all}}}\sigma_W. \quad (8)$$

Therefore, for user $\mathbf{u}^{(i)} \in \mathbf{U}^{\text{all}}$, the probability of successfully capturing him/her if he/she is guilty is

$$P_s^{(i)} = Q\left(\frac{h-\mu_t^{(i)}}{\sigma_n}\right) \quad (9)$$

and the probability of falsely accusing him/her if he/she is innocent is

$$P_{fa}^{(i)} = Q\left(\frac{h}{\sigma_n}\right). \quad (10)$$

The analysis of $P_d$, $P_{fp}$, $E[F_d]$ and $E[f_{fp}]$ is the same as that in Section III-A-1 and not repeated. It is clear from (9) and (8) that the higher the $\mu_t^{(i)}$ is, the better the traitor-tracing performance.

### B. Performance Comparison

This section compares the performance of the four detection statistics (4) and (8) when identifying colluders in $SC^{\text{all}}$. From the above analysis, for a given $h$ and a fixed $P_{fp}$, comparing $P_d$ of different detection statistics is equivalent to comparing their means.

For a colluder $i \in SC^{\text{all}}$, Fig. 2 shows an example of the means of the detection statistics in (4) and (8). In Fig. 2, we first generate independent vectors following Gaussian distribution $\mathcal{N}(0,1)$, and then apply Gram-Schmidt orthogonalization to generate orthogonal fingerprints for different users. The lengths of the fingerprints embedded in the base layer, enhancement layer 1 and enhancement layer 2 are $N_b = 50\,000$, $N_{e1} = 50\,000$ and $N_{e2} = 100\,000$, respectively. In Fig. 2, we fix the total number of colluders $K = 250$, and $K^b = 50$ of them receive the fingerprinted base layer only. Each point on the *X* axis corresponds to a unique triplet $(K^b, K^{e1}, K^{e2})$. The colluders follow the work in [15] to select the collusion parameters and generate a colluded copy with all three layers under the fairness constraints.

From Fig. 2, $TN_c^{(i)}$ in (4) has the best performance when more than 60% of the colluders receive a high-quality copy with all three layers. This is because in this scenario, $\mathbf{u}^{(i)}$'s fingerprints are spread all over the entire colluded copy $\mathbf{V}$, and $\mathbf{W}^{(i)}$'s energy is evenly distributed in the three layers of $\mathbf{V}$. Therefore, from detection theory [19], fingerprints extracted from all layers should be used during detection to improve the performance. When $K^{\text{all}}/K < 0.6$, due to the selection of the collusion parameters, a significant portion of $\mathbf{W}^{(i)}$'s energy is in the enhancement layer 2, while the other two layers of the colluded copy contain little information of $\mathbf{u}^{(i)}$'s identity. Thus, in this scenario, $TN_{e2}^{(i)}$ in (8) gives the best detection performance. Also, since larger $K^{\text{all}}$ introduces smaller fingerprint energy in enhancement layer 2 for $SC^{\text{all}}$, and the total number of colluders remains the same, thus smaller $K^b$ and $K^{b,e1}$ result in higher fingerprint energy for $SC^b$ and $SCb,e$ in base layer and enhancement layer 1. Therefore, $\alpha_1, \beta_1, \beta_2$ must be lower to ensure equal probability of being detected for every user. Hence, $\mu_{e1}$ and $\mu_b$ for $SC^{\text{all}}$ may increase as $K^{\text{all}}$ increases.

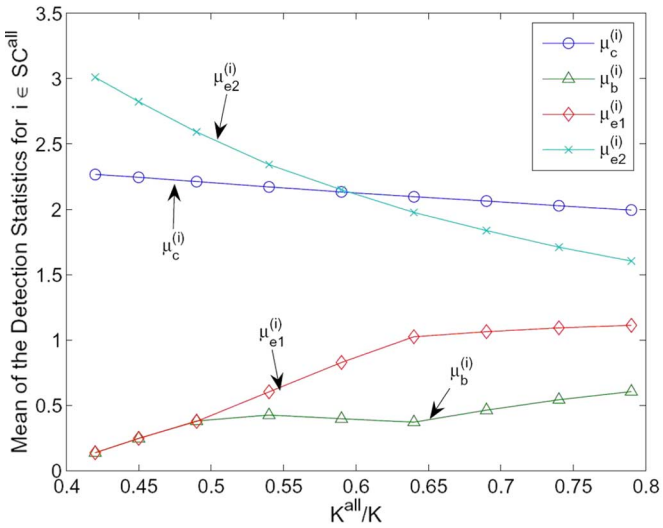



Fig. 2. Comparison of $\mu_c$ in (5), $\mu_{e2}^{(i)}$, $\mu_{e1}^{(i)}$, and $\mu_b^{(i)}$ in (9) for $i \in SC^{\text{all}}$. $(N_b, N_{e1}, N_{e2}) = (50\,000, 50\,000, 100\,000)$. $K = 250$ and $K^b = 50$. Each point on the *X* axis corresponds to a unique triplet $(K^b, K^{e1}, K^{e2})$. $F^c = F_b \cup F_{e1} \cup F_{e2}$.

### C. Colluder Identification With Side Information

For the four detection statistics in Section III-A, their traitor tracing capability is determined by their *statistical means*. The larger the statistical mean is, the better the performance. Note that from the above analysis, the collusion parameters ($\{\alpha_j\}$ and $\{\beta_l\}$ in the two-stage collusion model) determine the means of the detection statistics. Thus, if *side information about the statistical means* of different detection statistics (or equivalently, the collusion parameters) is available to the fingerprint detector, he/she should select the detection statistics that has the largest statistical mean to improve the traitor-tracing capability.

During the fingerprint detection and colluder identification process, the fingerprint detector should first examine the colluded copy and probe such side information, then select the best detection statistics and identify colluders. As an example, to identify colluders who receive all three layers, the key steps in probing the means of the detection statistics and selecting the optimum detection statistics are as follows:

- For every user $\mathbf{u}^{(i)}$ in $\mathbf{U}^{\text{all}}$, the detector first calculates $TN_c^{(i)}$, $TN_{e2}^{(i)}$, $TN_{e1}^{(i)}$ and $TN_b^{(i)}$ as in Section III-A, and obtains

$$\widehat{SC}_c^{\text{all}} = \left\{i : TN_c^{(i)} > h_t\right\}, \quad \widehat{SC}_{e2}^{\text{all}} = \left\{i : TN_{e2}^{(i)} > h_t\right\}$$
$$\widehat{SC}_{e1}^{\text{all}} = \left\{i : TN_{e1}^{(i)} > h_t\right\}, \quad \text{and}$$
$$\widehat{SC}_b^{\text{all}} = \left\{i : TN_b^{(i)} > h_t\right\} \quad (11)$$

  for a given $h_t$.

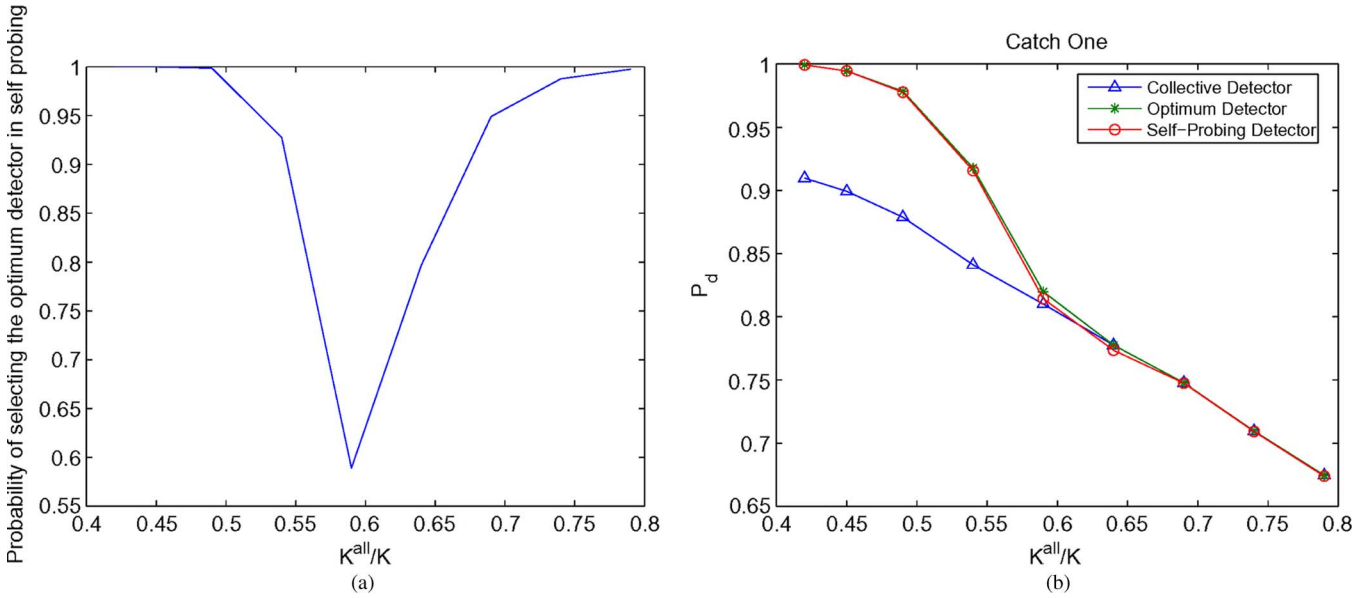



Fig. 3. Performance of the self-probing fingerprint detector for the example in Fig. 2. (a) Probability of selecting the optimum detection statistics when identifying colluders in $\mathbf{U}^{\text{all}}$. (b) $P_d$ of the collective detector, the optimum detector with perfect knowledge of the detection statistics' means, and the self-probing detector that probes the side information itself. $h_t$ is chosen to let $P_{fa}^{(i)} = 10^{-2}$ for an innocent user $i \notin SC$. $P_{fp} = 10^{-3}$. The result is based on 10 000 simulation runs.

- The detector combines the above four sets of estimated colluders in $\mathbf{U}^{\text{all}}$ and lets $\widehat{SC}^{\text{all}} = \widehat{SC}_c^{\text{all}} \cup \widehat{SC}_{e2}^{\text{all}} \cup \widehat{SC}_{e1}^{\text{all}} \cup \widehat{SC}_b^{\text{all}}$.
- Given $\widehat{SC}^{\text{all}}$, the detector estimates the means of the four detection statistics in Section III-A

$$\hat{\mu}_c = \sum_{k \in \widehat{SC}^{\text{all}}} \frac{TN_c^{(k)}}{|\widehat{SC}^{\text{all}}|}, \quad \hat{\mu}_{e2} = \sum_{k \in \widehat{SC}^{\text{all}}} \frac{TN_{e2}^{(k)}}{|\widehat{SC}^{\text{all}}|}$$
$$\hat{\mu}_{e1} = \sum_{k \in \widehat{SC}^{\text{all}}} \frac{TN_{e1}^{(k)}}{|\widehat{SC}^{\text{all}}|}, \quad \hat{\mu}_b = \sum_{k \in \widehat{SC}^{\text{all}}} \frac{TN_b^{(k)}}{|\widehat{SC}^{\text{all}}|}. \quad (12)$$

- The detector compares $\hat{\mu}_c$, $\hat{\mu}_{e2}$, $\hat{\mu}_{e1}$, and $\hat{\mu}_b$ and selects the detection statistics with the largest estimated mean. For example, the collective detector in (4) is chosen if $\hat{\mu}_c$ has the largest value.

When identifying colluders in $SC^{b,e1}$, the side information probing process is similar and not repeated. Then, the fingerprint detector follows Section III-A and estimates the identities of the colluders.

### D. Performance Analysis and Simulation Results

In our simulations, we simulate three different fingerprint detectors: the simple collective detector in (4); the optimum detector with perfect knowledge of the statistical means of the four detection statistics; and the self-probing detector, which first uses the algorithm in Section III-C to select the best detection statistics and then follows Section III-A to identify colluders.

The simulation setup is the same as that in Fig. 2. We choose the parameters based on the analysis in [15], which shows the total number of 250 colluders in a 750-user system is large enough to effectively reduce the fingerprint energy and reduce the probability of each colluder to be accused to around 10%, in which the fingerprint system can barely provide protection. Hence, under such tough scenario, we would test whether the proposed self-probing detector can provide better collusion resistance.

There are a total of $K = 250$ colluders, and $K^b = 50$ of them receive the fingerprinted base layer only. Each point on the $X$ axis in Fig. 3 corresponds to a unique triplet $(K^b, K^{b,e1}, K^{\text{all}})$. The colluders select $\{\alpha_k, \beta_l\}$ in the same way as in [15] and generate a colluded copy with all three layers. For each frame $j$ in the colluded copy, we adjust the power of the additive noise such that $\|\mathbf{n}_j\|^2 = \|\mathbf{W}_j^{(i)}\|^2$. Other values give the same trend.

Fig. 3(a) plots the probability that the proposed probing algorithm in Section III-C selects the optimum detection statistics when identifying colluders in $\mathbf{U}^{\text{all}}$. In the example in Fig. 2, we only choose between $TN^{(i)}$ and $TN_{e2}^{(i)}$ since $TN_{e1}^{(i)}$ and $TN_b^{(i)}$ never outperform the other two. From Fig. 3(a), the proposed probing algorithm selects the optimum detection statistics with probability 0.6 when $K^{\text{all}}/K \approx 0.6$; while in other scenarios, the detector always picks the best detection statistics. Note that from Fig. 2, when $K^{\text{all}}/K \approx 0.6$, $\mu_c$ and $\mu_{e2}^{(i)}$ have similar values and, therefore, $TN^{(i)}$ and $TN_{e2}^{(i)}$ have approximately the same performance. Consequently, in this scenario, choosing the sub-optimum detection statistics does not significantly deteriorate the detection performance. When $\mu_c$ and $\mu_{e2}^{(i)}$ differ significantly from each other, the self-probing detector always chooses the optimal detection statistics when identifying colluders in $\mathbf{U}^{\text{all}}$.

To evaluate the traitor-tracing performance of the proposed colluder identification algorithm with side information, we consider the catch one scenario, where the fingerprint detector aims to capture at least one colluder without falsely accusing any innocents. In this scenario, the criteria used to measure the performance is $P_d$ and $P_{fp}$. The analysis for other scenarios using other performance criteria is similar and gives the same trend. For a fixed $P_{fp} = 10^{-3}$, Fig. 3(b) shows $P_d$ of the three

detectors. From Fig. 3(b), utilizing side information about the means of different detection statistics can help the fingerprint detector significantly improve its performance, especially when $K^{\text{all}}/K$ is small and the colluders' fingerprints are not evenly distributed in the three layers of the colluded copy. Furthermore, from Fig. 3(b), when the difference between $\mu_c$ and $\mu_{e2}^{(i)}$ is large, the side information probing algorithm in Section III-C helps the detector choose the best detection statistics and achieve the optimal performance. When $\mu_c$ and $\mu_{e2}^{(i)}$ are approximately the same, the performance of the self-probing fingerprint detector is almost the same as that of the optimal detector with perfect knowledge of the means of the detection statistics, and the difference between these two is no larger than 0.005 and can be ignored.

### *E. Impact of Side Information on Fairness of Multi-User Collusion*

Without probing side information, the detector will always use all the frames collectively to identify the colluders, hoping that more frames will give him/her more information about colluders' identities. On the other side, colluders adjust the collusion parameters $\{\alpha_j\}$ and $\{\beta_l\}$ to seek the collective fairness. Under such circumstances, the colluders and the fingerprint detector reaches the *collective fairness equilibrium*. However, 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 they collude [20]. Thus, side information breaks the collective fairness equilibrium between the colluders and the fingerprint detector, and both sides need to search for a new equilibrium.

To demonstrate how side information breaks the collective fairness equilibrium, Fig. 4 shows each colluder's probability of being detected with the self-probing fingerprint detector. The simulation setup is the same as that in Fig. 3. In Fig. 4, colluders follow [15] to select the collusion parameters $\{\alpha_j\}$ and $\{\beta_l\}$ during the two-stage collusion, and we adjust the power of the additive noise such that $\|\mathbf{n}_j\|^2 = \|\mathbf{W}_j^{(i)}\|^2$ for each frame in the video sequence. From Fig. 4, when $K^{\text{all}}/K < 0.6$, those colluders who receive all three layers have a much larger probability of being detected than the others. In this example, during collusion, attackers only consider the collective detector in (5), and they select the parameters $\{\alpha_j\}$ and $\{\beta_l\}$ such that $\{TN_c^{(i)}\}$ in (5) have the same statistical mean for all attackers. However, during the colluder identification process, the fingerprint detector considers all possible detection strategies in Section III-A, probes side information about detection statistics, and uses the one that gives the best collusion resistance. Therefore, with the self-probing fingerprint detector in Section III-C, colluders have to find a new set of collusion parameters to ensure the equal risk of all attackers.

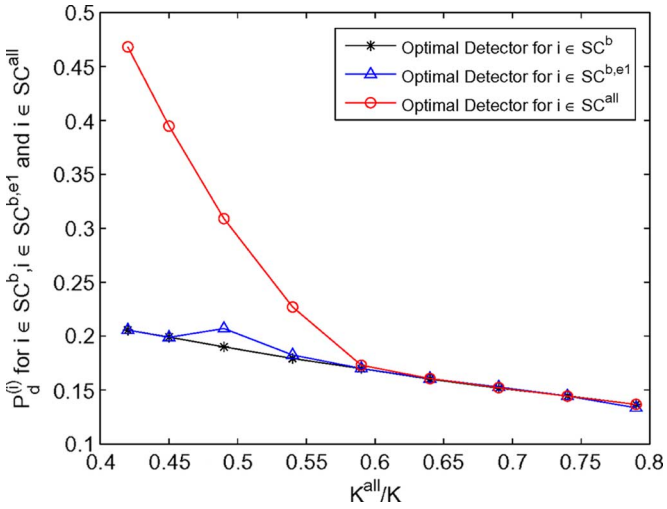



Fig. 4. Each colluder's probability of being detected ($P_s^{(i)}$) with the self-probing fingerprint detector. The simulation setup is the same as that in Fig. 3, and colluders follow [15] when selecting the collusion parameters $\{\alpha_k\}$ and $\{\beta_l\}$. The threshold $h$ is selected to satisfy $P_{fp} = 10^{-3}$. The results are based on 10 000 simulation runs.

## IV. Equilibrium of the Colluder-Detector Game With Side Information

In this section, we will model the behavior dynamics with side information between the two group of users in the multimedia fingerprinting social network as a two-person two-stage game. We formulate the equilibrium of this colluder-detector game as a min-max problem and find the optimal strategy of all users in the social network.

### *A. Game-Theoretical Modelling of Colluder-Detector Dynamics*

In the multimedia fingerprint social network, different members have different goals and utilities: the colluders mount attacks to generate the colluded copy for redistribution, and the forensic detector try to identify the colluders from the redistributed colluded copy. The colluders gain rewards by redistributing the colluded content and they take the risk to be caught by the digital rights enforcer. In this game, the colluders' gain is the detector's loss, thus the two group of members in the fingerprinting social network have totally conflicting objectives.

*1) Stackelberg Game Model:* To capture users' behavior in strategic situations, in which an individual's success in making choices depends on the choices of others, game theory [21], [22] is a useful tool to model the complex dynamics among multimedia social network members. Hence, to analyze the optimal strategies of both fingerprint detector and the colluders, we formulate the interaction between the two groups of social network members as a game with two players: the colluders acting as one single player and the fingerprint detector as the other.

- **Players**: There are two players: colluders who make decision first as the *leader*, followed by the fingerprint detector who apply detection as a *follower*.
- **Payoff Function Definition**: To analyze the dynamic between colluders and the forensic detector, we assume all the colluders have the same objectives and agree to share the same risk and reward. Therefore, during the fair collusion, every colluder has the same goal of minimizing his/her risk of being detected $P_s^{(i)}$ under the constraint that $\{P_s^{(i)}\}$ are the same for all colluders. Thus, a natural definition of colluder $i$'s payoff function is $\pi^C = 1 - P_s^{(i)}$, the probability that each colluder successfully removes traces of his/her fingerprint during collusion. From the detector's

point of view, the colluders' gain is the loss of the digital rights enforcer, so we can define the detector's payoff as $\pi^D = -\pi^C$.

- **Colluders' Strategies**: Each set of the collusion parameters $\{\alpha_1, \beta_1, \beta_2\}$ that achieves equal probability of detection for each colluder leads to one strategy for the colluders in the colluder-detector game.
- **Detector's Strategies**: As discussed in Section II-B-3, the detector's strategies include the collective detector, single-layer detector, and the self-probing detector. We assume the detector can probe the side information (the mean of the detection statistics) when he/she chooses the strategy.

In this game, there are multiple detection statistics that the fingerprint detector can use to identify colluders. However, by the analysis and simulation results shown in Section III-C, the self-probing detector can always achieve better or equal performance as all other detectors (collective detector and single-layer detector). Thus, to maximize his/her payoff, the fingerprint detector always probes side information about collusion and selects the detection statistics that has the largest chance of successfully capturing colluders. From the angle of game theoretical analysis, probing side-information is equivalent to observing the colluders' action. This scenario implies that the detector (follower in this game) can observe the colluders' action, and the colluders (leader) know that the detector observes their action. Hence, colluders as the leader have perfect knowledge of the detection strategies that the fingerprint detector will use, because the detector has no incentive to deviate from the self-probing detector. Therefore, the detector has no means of committing to a follower action that deviates from the self-probing detector which is the best response, and the colluders know this. Therefore, the colluder-detector game is a Stackelberg game [22] with perfect information.

*2) Equilibrium Analysis:* As shown in Fig. 4, with side information available to the fingerprint detector, the selected collusion parameters in [15] cannot guarantee the fairness of collusion. Therefore, the colluders need to find new sets of collusion parameters to achieve fairness.

With the proposed self-probing fingerprint detection process in Section III-C, for every type of collusion, the fingerprint detector will always choose the detection statistics that gives the best traitor-tracing performance which can be illustrated as the game tree shown in Fig. 5. In this game, assuming that there are N possible collusion strategies under the fairness constraint, the colluders first choose the collusion strategy, and then the fingerprint detector selects the optimal detection statistics.

Since the follower (detector) can observe the leader's (colluders') strategy, the game model can be solved by backward induction. The backward induction starts from the last stage of the game, which is the detector's strategy. As shown in Section III-C, the self-probing detector is the optimal strategy for all the fair collusion. Hence, we can move forward to the previous stage in the game, which is the colludes' strategy. Since both the colluders and the fingerprint detector know that the optimal detection statistics will be used to identify colluders, once attackers determine the collusion strategy, their payoff is fixed and the colluders can accurately estimate their payoff. The colluders consider what the best response of the detector is, i.e., how the detector will respond once he/she observes the leader's strategy. The colluders then pick a strategy that maximizes its payoff, anticipating the predicted response of the detector. Hence, during collusion, colluders should consider the worst case scenario where the fingerprint detector always makes the right decision when selecting which detection statistics to use. They select the collusion parameters to minimize their risk under the constraint that all colluders have the same probability of being detected. Thus, the equilibrium of this game can be modelled as a *min-max problem*.

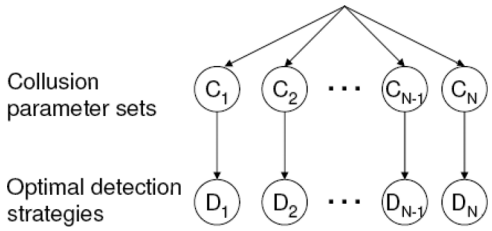



Fig. 5. Game tree illustration of the colluder-detector dynamics. $C_1, C_2, \cdots, C_N$ are the N possible sets of collusion parameters that achieve absolute fairness when the fingerprint detector uses the optimal detection statistics to identify colluders; while $D_1, D_2, \cdots, D_N$ are the corresponding optimal fingerprint detection strategies. For the example of $(K^b, K^{b,e1}, K^{\text{all}}) = (50, 25, 175)$ in Section IV-E, $\mathrm{N} = 3$, $C_1$ set of parameters satisfies (37), $C_2$ set of parameters satisfies (38), and $C_3$ set of parameters satisfies (39). In $D_1$, the fingerprint detector uses $TN_b^{(i)}$ for $i \in \mathbf{U}^{b,e1}$ and $TN_c^{(j)}$ for $j \in \mathbf{U}^{\text{all}}$. In $D_2$, the fingerprint detector uses $TN_{e1}^{(i)}$ for $i \in \mathbf{U}^{b,e1}$ and $TN_c^{(j)}$ for $j \in \mathbf{U}^{\text{all}}$. In $D_3$, the fingerprint detector uses $TN_c^{(i)}$ for $i \in \mathbf{U}^{b,e1}$ and $TN_c^{(j)}$ for $j \in \mathbf{U}^{\text{all}}$.

As we discussed in Section III-E, without side information, the colluders and the detector achieve the collective fairness equilibrium: the fingerprint detector uses the collective detection statistics in (4), and the colluders select the collusion parameter as in [15] to ensure the same risk under the collective detector. Probing and utilizing side information moves the equilibrium of the colluder-detector game from the collective one to the min-max solution as discussed in Section IV-C.

### *B. Min-Max Problem Formulation of the Equilibrium*

For each user $\mathbf{u}^{(i)}$, define $\mathfrak{D}^{(i)}$ as the set including all possible detection statistics that can be used to measure the similarity between the extracted fingerprint $\mathbf{Y}$ and $\mathbf{u}^{(i)}$'s fingerprint $\mathbf{W}^{(i)}$. For example, $\mathfrak{D}^{(i)} = \{TN_c^{(i)}, TN_{e2}^{(i)}, TN_{e1}^{(i)}, TN_b^{(i)}\}$ for a colluder $i \in SC^{\text{all}}$ who receives all three layers, while $\mathfrak{D}^{(i)} = \{TN_c^{(i)}, TN_{e1}^{(i)}, TN_b^{(i)}\}$ for user $i \in SC^{b,e1}$ who receives a medium resolution copy. Define $P_s^{(i)}(\mathfrak{D}^{(i)}, \{\alpha_k, \beta_l\})$ as the probability that colluder $\mathbf{u}^{(i \in SC)}$ is captured by the digital rights enforcer.

Consequently, we can model the problem as a min-max problem:

$$\begin{aligned} &\min_{\{\alpha_k,\beta_l\}} \max_{\mathfrak{D}^{(i)}} P_s^{(i)} \left(\mathfrak{D}^{(i)}, \{\alpha_k, \beta_l\}\right) \\ &\text{s.t.} \max_{\mathfrak{D}^{(i_1)}} P_s^{(i_1)} \left(\mathfrak{D}^{(i_1)}, \{\alpha_k, \beta_l\}\right) \\ &\quad = \max_{\mathfrak{D}^{(i_2)}} P_s^{(i_2)} \left(\mathfrak{D}^{(i_2)}, \{\alpha_k, \beta_l\}\right), \ \forall i_1, i_2 \in SC. \quad (13) \end{aligned}$$

From the analysis in the previous section, for a given threshold $h$ and fixed $\sigma_n^2$, $P_s^{(i)}$ is determined by the mean of the detection

statistics that are used. Therefore, for colluder $i_1 \in SC^b$, $i_2 \in SC^{b,e1}$ and $i_3 \in SC^{\text{all}}$, (13) can be simplified to

$$\begin{aligned}&\min_{\{\alpha_k,\beta_l\}} \mu = \mu_{\max}^{(i_1)} = \mu_{\max}^{(i_2)} = \mu_{\max}^{(i_3)}\\ &\text{s.t.}\quad 0 \le \alpha_k \le 1, 0 \le \beta_l \le 1\end{aligned}$$

where

$$\begin{aligned}\mu_{\max}^{(i_1)} &= \mu_c^{(i_1)}\\ \mu_{\max}^{(i_2)} &= \max\left\{\mu_b^{(i_2)}, \mu_{e1}^{(i_2)}, \mu_c^{(i_2)}\right\}\end{aligned}$$

and

$$\mu_{\max}^{(i_3)} = \max\left\{\mu_b^{(i_3)}, \mu_{e1}^{(i_3)}, \mu_{e2}^{(i_3)}, \mu_c^{(i_3)}\right\}. \tag{14}$$

In (14)

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

and

$$\mu_c^{(i_3)} = \frac{(1-\beta_1-\beta_2)N_b + (1-\alpha_1)N_{e1} + N_{e2}}{K^{\text{all}}\sqrt{N_b + N_{e1} + N_{e2}}}\sigma_W \tag{15}$$

from the analysis in Section III-A.

Given $(K^b, K^{b,e1}, K^{\text{all}})$ and $(N_b, N_{e1}, N_{e2})$, for colluder $i_1 \in SC^b$, $i_2 \in SC^{b,e1}$ and $i_3 \in SC^{\text{all}}$ who receive fingerprinted copies of different resolutions, they first find all possible sets of collusion parameters $\{\alpha_k, \beta_l\}$ that satisfy $\mu_{\max}^{(i_1)} = \mu_{\max}^{(i_2)} = \mu_{\max}^{(i_3)}$. Then, they select the one that gives them the minimum risk of being detected.

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

To solve the problem of (14), we first need to analyze $\mu_{\max}^{(i)}$ for each colluder $\mathbf{u}^{(i)}$ and study which detection statistics have the maximum mean under which condition.

*1) For Colluder $i \in SC^{b,e1}$:* For colluder $i \in SC^{b,e1}$ who receives a medium resolution copy, there are three possibilities: $\mu_{\max}^{(i)} = \mu_b^{(i)}$, $\mu_{\max}^{(i)} = \mu_{e1}^{(i)}$ and $\mu_{\max}^{(i)} = \mu_c^{(i)}$.

$\mu_{\max}^{(i)} = \mu_b^{(i)}$: If $\mu_{\max}^{(i)} = \mu_b^{(i)}$, then $\mu_b^{(i)} \ge \mu_{e1}^{(i)}$ and $\mu_b^{(i)} \ge \mu_c^{(i)}$. Thus, from (15)

$$\mu_{\max}^{(i)} = \mu_b^{(i)} \text{ if and only if } \beta_2 \ge \frac{\alpha_1 N_{e1}}{\sqrt{N_b}(\sqrt{N_b + N_{e1}} - \sqrt{N_b})}. \tag{16}$$

$\mu_{\max}^{(i)} = \mu_{e1}^{(i)}$: In this case, $\mu_{e1}^{(i)} \ge \mu_b^{(i)}$ and $\mu_{e1}^{(i)} \ge \mu_c^{(i)}$. Thus,

$$\begin{aligned}&\mu_{\max}^{(i)} = \mu_{e1}^{(i)} \quad \text{if and only if}\\ &\beta_2 \le \frac{\alpha_1\sqrt{N_{e1}}\left(\sqrt{(N_b + N_{e1})} - \sqrt{N_{e1}}\right)}{N_b}.\end{aligned} \tag{17}$$

$\mu_{\max}^{(i)} = \mu_c^{(i)}$: This scenario happens if $\mu_c^{(i)} \ge \mu_b^{(i)}$ and $\mu_c^{(i)} \ge \mu_{e1}^{i)}$. Following the same analysis as in the previous two scenarios as in Appendix, $\mu_{\max}^{(i)} = \mu_c^{(i)}$ if and only if

$$\begin{aligned}&\frac{\alpha_1\sqrt{N_{e1}}\left(\sqrt{(N_b + N_{e1})} - \sqrt{N_{e1}}\right)}{N_b} \le \beta_2\\ &\le \frac{\alpha_1 N_{e1}}{\sqrt{N_b}(\sqrt{N_b + N_{e1}} - \sqrt{N_b})}.\end{aligned} \tag{18}$$

Detailed proofs of (16), (17), (18) are in Appendix A, B, C, respectively.

*2) For Colluder $i \in SC^{\text{all}}$:* For Colluder $i \in SC^{\text{all}}$, if the colluded copy includes all three layer, there are four possibilities for $\mu_{\max}^{(i)}$: $\mathbf{u}_{\max}^{(i)} = \mathbf{u}_b^{(i)}$, $\mathbf{u}_{\max}^{(i)} = \mathbf{u}_{e1}^{(i)}$, $\mathbf{u}_{\max}^{(i)} = \mathbf{u}_{e2}^{(i)}$, and $\mathbf{u}_{\max}^{(i)} = \mathbf{u}_c^{(i)}$.

$\mathbf{u}_{\max}^{(i)} = \mathbf{u}_b^{(i)}$: Following the same analysis as the previous section

$$\begin{aligned}\mu_{\max}^{(i)} = \mu_b^{(i)} \Leftrightarrow \mu_b^{(i)} \ge \mu_{e1}^{(i)}, \quad \mu_b^{(i)} \ge \mu_{e2}^{(i)}, \quad \text{and}\\ \mu_b^{(i)} \ge \mu_c^{(i)}\end{aligned}$$

where

$$\begin{aligned}\mu_b^{(i)} \ge \mu_{e1}^{(i)} &\Leftrightarrow \beta_1 + \beta_2 \le 1 - (1-\alpha_1)\frac{\sqrt{N_{e1}}}{\sqrt{N_b}}\\ \mu_b^{(i)} \ge \mu_{e2}^{(i)} &\Leftrightarrow \beta_1 + \beta_2 \le 1 - \frac{\sqrt{N_{e2}}}{\sqrt{N_b}}\end{aligned}$$

and

$$\begin{aligned}\mu_b^{(i)} \ge \mu_c^{(i)} &\Leftrightarrow \beta_1 + \beta_2\\ &\le 1 - \frac{(1-\alpha_1)N_{e1} + N_{e2}}{\sqrt{N_b}(\sqrt{N_b + N_{e1} + N_{e2}} - \sqrt{N_b})}.\end{aligned} \tag{19}$$

Note that we have the constraint $0 \le \beta_1, \beta_2 \le \beta_1 + \beta_2 \le 1$ in (14) when selecting the collusion parameters. Therefore, from (19), in order to satisfy $\mu_b^{(i)} \ge \mu_{e2}^{(i)}$ and let $\mu_b^{(i)} = \max\{\mu_b^{(i)}, \mu_{e1}^{(i)}, \mu_{e2}^{(i)}, \mu_c^{(i)}\}$, $N_{e2} \le N_b$ must be true. This observation explains why in the example shown in Fig. 2 where $N_{e2} = 2N_b$, among the four detection statistics, $TN_b^{(i)}$ never achieves the best performance.

$\mathbf{u}_{\max}^{(i)} = \mathbf{u}_{e1}^{(i)}$: In this scenario

$$\begin{aligned}\mu_{\max}^{(i)} = \mu_{e1}^{(i)} \Leftrightarrow \mu_{e1}^{(i)} > \mu_b^{(i)}, \quad \mu_{e1}^{(i)} \ge \mu_{e2}^{(i)}, \quad \text{and}\\ \mu_{e1}^{(i)} \ge \mu_c^{(i)}\end{aligned}$$

where

$$\begin{aligned}\mu_{e1}^{(i)} \ge \mu_b^{(i)} &\Leftrightarrow \alpha_1 \ge 1 - (1-\beta_1-\beta_2)\frac{\sqrt{N_{e2}}}{\sqrt{N_{e1}}}\\ \mu_{e1}^{(i)} \ge \mu_{e2}^{(i)} &\Leftrightarrow \alpha_1 \le 1 - \frac{\sqrt{N_{e2}}}{\sqrt{N_{e1}}}\end{aligned}$$

and

$$\begin{aligned}&\mu_{e1}^{(i)} \ge \mu_c^{(i)} \Leftrightarrow\\ &\alpha_1 \le 1 - \frac{(1-\beta_1-\beta_2)N_b + N_{e2}}{\sqrt{N_{e1}}(\sqrt{N_b + N_{e1} + N_{e2}} - \sqrt{N_{e1}})}.\end{aligned} \tag{20}$$

From (20), $N_{e2} \leq N_{e1}$ must hold in order to let $\mu_{e1}^{(i)} = \max\{\mu_b^{(i)}, \mu_{e1}^{(i)}, \mu_{e2}^{(i)}, \mu_c^{(i)}\}$, which is the reason that in Fig. 2 with $N_{e2} = 2N_{e1}$, $TN_{e2}^{(i)}$ never gives the best traitor-tracing performance.

$\mathbf{u}_{\max}^{(i)} = \mathbf{u}_{e2}^{(i)}$: See (21) at the bottom of the page.

$\mathbf{u}_{\max}^{(i)} = \mathbf{u}_c^{(i)}$: Following the same analysis as in the previous section, see (22) at the bottom of the page.

### D. Analysis of the Feasible Set

Given the above analysis on $\mu_{\max}^{(i)}$, for each given $(N_b, N_{e1}, N_{e2})$ and $(K^b, K^{b,e1}, K^{\text{all}})$, the next step is to study how attackers achieve fairness of collusion and let $\mu_{\max}^{(i)}$ be the same for all colluders. This section investigates the constraints on collusion to ensure the fair play of the attack.

Without loss of generality, in this section, we use $N_b : N_{e1} : N_{e2} = 1 : 1 : 2$ as an example to illustrate how colluders achieve fairness of the attack and analyze the constraints on collusion. We assume that colluders generate a high-resolution colluded copy including all three layers. In this scenario, from the analysis in the above 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 $i_3 \in SC^{\text{all}}$ who receives all three layers, $\mu_{\max}^{(i_3)}$ equals either $\mu_{e1}^{(i_3)}$ or $\mu_c^{(i_3)}$, and $\mu_{\max}^{(i_3)} \neq \mu_b^{(i_3)}$ and $\mu_{\max}^{(i_3)} \neq \mu_{e1}^{(i_3)}$. Thus, there are a total of 6 possible scenarios, which are as follows:

1) $\mu_{\max}^{(i_2)} = \mu_b^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_{e2}^{(i_3)}$ for $i_3 \in SC^{\text{all}}$
2) $\mu_{\max}^{(i_2)} = \mu_{e1}^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_{e2}^{(i_3)}$ for $i_3 \in SC^{\text{all}}$
3) $\mu_{\max}^{(i_2)} = \mu_c^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_{e2}^{(i_3)}$ for $i_3 \in SC^{\text{all}}$
4) $\mu_{\max}^{(i_2)} = \mu_b^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_c^{(i_3)}$ for $i_3 \in SC^{\text{all}}$
5) $\mu_{\max}^{(i_2)} = \mu_{e1}^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_c^{(i_3)}$ for $i_3 \in SC^{\text{all}}$
6) $\mu_{\max}^{(i_2)} = \mu_c^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_c^{(i_3)}$ for $i_3 \in SC^{\text{all}}$

*1) Scenario 1 $\mu_{\max}^{(i_2)} = \mu_b^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_{e2}^{(i_3)}$ for $i_3 \in SC^{\text{all}}$:* In this scenario, for three colluders $i_1 \in SC^b$, $i_2 \in SC^{b,e1}$ and $i_3 \in SC^{\text{all}}$, from (15)

$$\mu^{(i_1)} = \frac{\beta_1\sqrt{N_b}}{K^b}\sigma_W,\ \mu_{\max}^{(i_2)} = \frac{\beta_2\sqrt{N_b}}{K^{b,e1}}\sigma_W, \text{ and}$$
$$\mu_{\max}^{(i_3)} = \frac{\sqrt{N_{e2}}}{K^{\text{all}}}\sigma_W. \tag{23}$$

To achieve fairness of the attack, colluders select the collusion parameters $\{\alpha_k, \beta_l\}$ such that $\mu^{(i_1)} = \mu_{\max}^{(i_2)} = \mu_{\max}^{(i_3)}$. Therefore, we have

$$\beta_1 = \frac{\sqrt{N_{e2}}}{\sqrt{N_b}}\frac{K^b}{K^{\text{all}}} = \sqrt{2}\frac{K^b}{K^{\text{all}}}, \quad \text{and}$$
$$\beta_2 = \frac{K^{b,e1}}{K^b}\beta_1 = \sqrt{2}\frac{K^{b,e1}}{K^{\text{all}}}. \tag{24}$$

In this scenario, since $\mu_b^{(i_2)}$ is the largest among $\{\mu_b^{(i_2)}, \mu_{e1}^{(i_2)}, \mu_c^{(i_2)}\}$, from (16), the selected collusion parameters must satisfy

$$\alpha_1 \leq \beta_2\frac{\sqrt{N_b}(\sqrt{N_b + N_{e1}} - \sqrt{N_b})}{N_{e1}}$$
$$= \frac{\sqrt{2N_b}(\sqrt{N_b + N_{e1}} - \sqrt{N_b})}{N_{e1}}\frac{K^{b,e1}}{K^{\text{all}}} \triangleq A. \tag{25}$$

$A = (2 - \sqrt{2})K^{b,e1}/K^{\text{all}}$ in our example of $N_b : N_{e1} : N_{e2} = 1 : 1 : 2$. Define $R^b = K^b/K$, $R^{b,e1} = K^{b,e1}/K$ and $R^{\text{all}} = K^{\text{all}}/K$ as the percentages of colluders who are in $SC^b$, $SC^{b,e1}$, and $SC^{\text{all}}$, respectively. Following the same analysis, scenario 1 will happen if only if

$$\frac{\sqrt{2}}{1+\sqrt{2}} \leq R^{\text{all}} \leq \min\left\{\frac{2 - (2-\sqrt{2})R^b}{6 - 2\sqrt{2}}, 1 - R^b\right\}. \tag{26}$$

---

$$\mu_{\max}^{(i)} = \mu_{e2}^{(i)} \Leftrightarrow \alpha_1 \geq 1 - \frac{\sqrt{N_{e2}}}{\sqrt{N_{e1}}}$$

and

$$\beta_1 + \beta_2 \geq 1 + \frac{(1-\alpha_1)N_{e1} - \sqrt{N_{e2}}(\sqrt{N_b + N_{e1} + N_{e2}} - \sqrt{N_{e2}})}{N_b} \tag{21}$$

---

$$\mu_{\max}^{(i)} = \mu_c^{(i)} \Leftrightarrow \beta_1 + \beta_2 \geq 1 - \frac{(1-\alpha_1)N_{e1} + N_{e2}}{\sqrt{N_b}(\sqrt{N_b + N_{e1} + N_{e2}} - \sqrt{N_b})}$$
$$\beta_1 + \beta_2 \leq 1 - \frac{(1-\alpha_1)\sqrt{N_{e1}}(\sqrt{N_b + N_{e1} + N_{e2}} - \sqrt{N_{e1}}) - N_{e2}}{N_b}$$

and

$$\beta_1 + \beta_2 \leq 1 + \frac{(1-\alpha_1)N_{e1} - \sqrt{N_{e2}}(\sqrt{N_b + N_{e1} + N_{e2}} - \sqrt{N_{e2}})}{N_b} \tag{22}$$

To summarize, if $(R^b, R^{b,e1}, R^{\text{all}})$ satisfies (26), colluders can achieve fairness of the attack by following, and the resulting feasible set is the black area in Fig. 6(a). 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 $i \in SC^{\text{all}}$. Fig. 6(a) plots all the $(R^b, R^{b,e1}, R^{\text{all}})$ that satisfy (26). The black area in Fig. 6(b) to (f) shows the feasible region of scenario 2 to 5, respectively (the analysis of scenario 2 5 is in Appendix D). Given any triple $(K_b, K_{b,e1}, K_{\text{all}})$ describing the number of colluders who have lowest to highest resolution copies, Fig. 6 provides the feasible strategies of collusion.

*2) Scenario 2 $\mu_{\max}^{(i_2)} = \mu_{e1}^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_{e2}^{(i_3)}$ for $i_3 \in SC^{\text{all}}$:* Following the same analysis as in Section IV-D-1, for the example of $N_b : N_{e1} : N_{e2} = 1 : 1 : 2$, if $(R^b, R^{b,e1}, R^{\text{all}})$ satisfied

$$\max\left\{\sqrt{2}R^b, (2-\sqrt{2})(1-R^b)\right\} \le R^{\text{all}} \le \min\left\{\frac{2-(2-\sqrt{2})R^b}{6-2\sqrt{2}}, \frac{\sqrt{2}-\sqrt{2}R^b}{3-\sqrt{2}}, 1-R^b\right\} \quad (27)$$

colluders can guarantee the equal risk of all attackers by selecting

$$\alpha_1 = \sqrt{2}\frac{K^{b,e1}}{K^{\text{all}}}, \quad \beta_1 = \sqrt{2}\frac{K^b}{K^{\text{all}}}$$
$$\text{and} \quad 4-\sqrt{2}-\sqrt{2}\frac{K}{K^{\text{all}}} \le \beta_2 \le \min\left\{1-\sqrt{2}\frac{K^b}{K^{\text{all}}}, (2-\sqrt{2})\frac{K^{b,e1}}{K^{\text{all}}}\right\}. \quad (28)$$

Fig. 6(b) shows all the $(R^b, R^{b,e1}, R^{\text{all}})$ that satisfy (27).

*3) Scenario 3 $\mu_{\max}^{(i_2)} = \mu_c^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_{e2}^{(i_3)}$ for $i_3 \in SC^{\text{all}}$:* Given $N_b : N_{e1} : N_{e2} = 1 : 1 : 2$, if $(R^b, R^{b,e1}, R^{\text{all}})$ satisfies

$$\max\left\{\frac{2-(2-\sqrt{2})R^b}{4}, \frac{(2-\sqrt{2})+(2\sqrt{2}-2)R^b}{3-\sqrt{2}}\right\} \le R^{\text{all}} \le \left\{\frac{2-(2-\sqrt{2})R^b}{6-2\sqrt{2}}, 1-R^b\right\} \quad (29)$$

and colluders select

$$\beta_1 = \sqrt{2}\frac{K^b}{K^{\text{all}}}$$
$$\max\left\{2\frac{K^{b,e1}}{K^{\text{all}}}-1, (2-\sqrt{2})\frac{K^{b,e1}}{K^{\text{all}}}\right\} \le \beta_2 \le \min\left\{\sqrt{2}\frac{K^{b,e1}}{K^{\text{all}}}, 1-\sqrt{2}\frac{K^b}{K^{\text{all}}}\right\}$$

and

$$\alpha_1 = 2\frac{K^{b,e1}}{K^{\text{all}}} - \beta_2 \quad (30)$$

then $\mu_{\max}^{(i_2)} = \mu_c^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_{e2}^{(i_3)}$ for $i_3 \in SC^{\text{all}}$, and all colluders have the same probability of being detected by the fingerprint detector. Fig. 6(c) plots all the $(R^b, R^{b,e1}, R^{\text{all}})$ that satisfy (29).

*4) Scenario 4 $\mu_{\max}^{(i_2)} = \mu_b^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_c^{(i_3)}$ for $i_3 \in SC^{\text{all}}$:* Given $N_b : N_{e1} : N_{e2} = 1 : 1 : 2$, if

$$\max\left\{2-\sqrt{2}, \frac{4-\sqrt{2}+(\sqrt{2}-1)R^b}{6-\sqrt{2}}\right\} \le R^{\text{all}} \le 1-R^b \quad (31)$$

holds, by choosing the collusion parameters as

$$\beta_1 \ge \max\left\{\frac{4K^b}{\sqrt{2}K-(\sqrt{2}-1)K^b+(2-\sqrt{2})K^{\text{all}}}, \frac{3K^b}{K+K^{\text{all}}}, \frac{\sqrt{2}K^b}{K^{\text{all}}}\right\}$$
$$\beta_1 \le \min\left\{\frac{K^b}{K-K^{\text{all}}}, \frac{4K^b}{K+K^{\text{all}}}\right\}$$
$$\beta_2 = \frac{K^{b,e1}}{K^b}\beta_1, \quad \text{and} \quad \alpha_1 = 4-\frac{K+K^{\text{all}}}{K^b}\beta_1 \quad (32)$$

colluders achieve fairness of collusion and $\mu_{\max}^{(i_2)} = \mu_b^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_c^{(i_3)}$ for $i_3 \in SC^{\text{all}}$ in this scenario. Fig. 6(d) plots all the $(R^b, R^{b,e1}, R^{\text{all}})$ that satisfy (31).

*5) Scenario 5 $\mu_{\max}^{(i_2)} = \mu_{e1}^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_c^{(i_3)}$ for $i_3 \in SC^{\text{all}}$:* Here, under the constraint that $(R^b, R^{b,e1}, R^{\text{all}})$ satisfies

$$\max\left\{4R^b-1, \sqrt{2}R^b, \frac{4-\sqrt{2}-(5-\sqrt{2})R^b}{6-\sqrt{2}}, \frac{\sqrt{2}}{4-\sqrt{2}}\right\} \le R^{\text{all}} \le 1-R^b \quad (33)$$

all colluders have the same probability of being detected if they select

$$\beta_1 \ge \max\left\{\frac{4K^b}{\sqrt{2}K-(\sqrt{2}-1)K^b+(2-\sqrt{2})K^{\text{all}}}, \frac{3K^b}{K+K^{\text{all}}-K^b}, \frac{\sqrt{2}K^b}{K^{\text{all}}}\right\}$$
$$\beta_1 \le \min\left\{\frac{K^b}{K^{b,e1}}, \frac{4K^b}{K+K^{\text{all}}}\right\}$$
$$\beta_2 = 4-\frac{K+K^{\text{all}}}{K^b}\beta_1, \quad \text{and} \quad \alpha_1 = \frac{K^{b,e1}}{K^b}\beta_1 \quad (34)$$

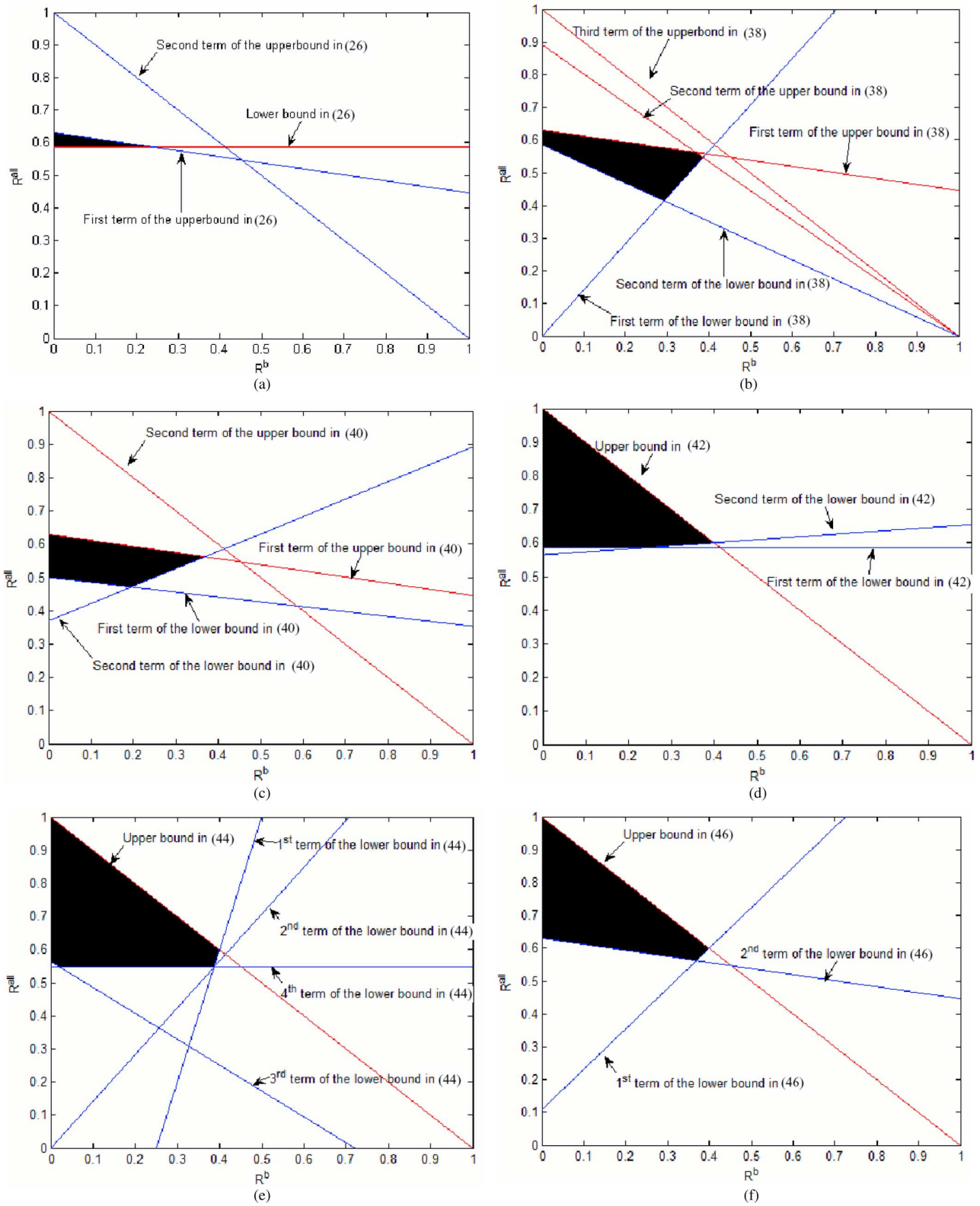



Fig. 6. $(R^b, R^{b,e1}, R^{\text{all}})$ that satisfy (a): (26) in Scenario 1. (b): (27) in Scenario 2. (c): (29) in Scenario 3. (d): (31) in Scenario 4. (e): (33) in Scenario 5, and (f): (35) in Scenario 6. Here, $N_b : N_{e1} : N_{e2} = 1 : 1 : 2$.

during collusion. In this scenario, $\mu_{\max}^{(i_2)} = \mu_{e1}^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_c^{(i_3)}$ for $i_3 \in SC^{\text{all}}$. Fig. 6(e) shows all the $(R^b, R^{b,e1}, R^{\text{all}})$ that satisfy (33).

*6) Scenario 6 $\mu_{\max}^{(i_2)} = \mu_c^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_c^{(i_3)}$ for $i_3 \in SC^{\text{all}}$:* If $(R^b, R^{b,e1}, R^{\text{all}})$ satisfies the constraint

$$\max\left\{\frac{3\sqrt{2}-4-(3\sqrt{2}-7)R^b}{3\sqrt{2}-2}, \frac{\sqrt{2}-(\sqrt{2}-1)R^b}{3\sqrt{2}-2}\right\} \leq R^{\text{all}} \leq 1-R^b \quad (35)$$

and if the selected parameters are

$$\beta_1 = \frac{4K^b}{\sqrt{2}K - (\sqrt{2}-1)K^b + (2-\sqrt{2})K^{\text{all}}}$$

$$\alpha_1 \geq \max\left\{\frac{3\sqrt{2}K^{b,e1} + 3K^b - 2K^{\text{all}}}{\sqrt{2}K - (\sqrt{2}-1)K^b + (2-\sqrt{2})K^{\text{all}}}, \frac{4(\sqrt{2}-1)K^{b,e1}}{\sqrt{2}K - (\sqrt{2}-1)K^b + (2-\sqrt{2})K^{\text{all}}}\right\}$$

$$\alpha_1 \leq \frac{4K^{b,e1}}{\sqrt{2}K - (\sqrt{2}-1)K^b + (2-\sqrt{2})K^{\text{all}}}$$

and

$$\beta_2 + \alpha_1 = \frac{4\sqrt{2}K^{b,e1}}{\sqrt{2}K - (\sqrt{2}-1)K^b + (2-\sqrt{2})K^{\text{all}}} \tag{36}$$

then all colluders have the same risk and $\mu_{\max}^{(i_2)} = \mu_c^{(i_2)}$ for $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_c^{(i_3)}$ for $i_3 \in SC^{\text{all}}$. Fig. 6(f) plots all the $(R^b, R^{b,e1}, R^{\text{all}})$ that satisfy (35).

### *E. Min-Max Solution*

Given the analysis in Section IV-D, for three colluders $i_1 \in SC^b, i_2 \in SC^{b,e1}$ and $i_3 \in SC^{\text{all}}$, the colluders first identify all the possible collusion parameters $\{\alpha_l, \beta_k\}$ that satisfy $\mu_{\max}^{(i_1)} = \mu_{\max}^{b,e1} = \mu_{\max}^{\text{all}}$ under the constraints, and then select the one that gives them the minimum risk of being detected.

To demonstrate this process, we use the system setup in Fig. 3 as an example, where the lengths of the fingerprints embedded in the base layer, the enhancement layer 1 and the enhancement layer 2 are $N_b = 5000$, $N_{e1} = 5000$, and $N_{e2} = 10000$, respectively. When generating fingerprints, we first generate independent Gaussian vectors following distribution $\mathcal{N}(0,1)$ and then apply Gram-Schmidt orthogonalization to produce fingerprints that have equal energies and are strictly orthogonal to each other.

Assume that there are a total of $K = 250$ colluders. Among the 250 colluders, if $K^b = 50$, $K^{b,e1} = 25$, and $K^{\text{all}} = 175$, i.e., $(R^b, R^{b,e1}, R^{\text{all}}) = (0.2, 0.1, 0.7)$, then from Section IV-D, $(R^b, R^{b,e1}, R^{\text{all}})$ satisfies (31) in Scenario 4 as in Appendix, the constraint (33) in Scenario 5, and the one (35) in Scenario 6.

- Since $(R^b, R^{b,e1}, R^{\text{all}})$ satisfies the constraint (31) in Scenario 4, colluders can guarantee the equal risk of all colluders if they choose

$$\beta_1 \geq \max\left\{\frac{4K^b}{\sqrt{2}K - (\sqrt{2}-1)K^b + (2-\sqrt{2})K^{\text{all}}}, \frac{3K^b}{K + K^{\text{all}}}, \frac{\sqrt{2}K^b}{K^{\text{all}}}\right\} = 0.4594$$

$$\beta_1 \leq \min\left\{\frac{K^b}{K - K^{\text{all}}}, \frac{4K^b}{K + K^{\text{all}}}\right\} = 0.4706$$

$$\beta_2 = \frac{K^{b,e1}}{K^b}\beta_1, \quad \text{and} \quad \alpha_1 = 4 - \frac{K + K^{\text{all}}}{K^b}\beta_1. \tag{37}$$

  Here, $\mu_{\max}^{(i_2)} = \mu_b^{(i_2)}$ for colluder $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_c^{(i_3)}$ for colluder $i_3 \in SC^{\text{all}}$. For any colluder $i \in SC$, $\mu_{\max}^{(i)}$ has the smallest possible value of 2.0545 when $\beta_1 = 0.4594$, $\beta_2 = 0.2297$, and $\alpha_1 = 0.0951$.

- Following (34), when colluders select parameters

$$\beta_1 \geq \max\left\{\frac{4K^b}{\sqrt{2}K - (\sqrt{2}-1)K^b + (2-\sqrt{2})K^{\text{all}}}, \frac{3K^b}{K + K^{\text{all}} - K^b}, \frac{\sqrt{2}K^b}{K^{\text{all}}}\right\} = 0.4594$$

$$\beta_1 \leq \min\left\{\frac{K^b}{K^{b,e1}}, \frac{4K^b}{K + K^{\text{all}}}\right\} = 0.4706$$

$$\beta_2 = 4 - \frac{K + K^{\text{all}}}{K^b}\beta_1, \quad \text{and} \quad \alpha_1 = \frac{K^{b,e1}}{K^b}\beta_1 \tag{38}$$

  they have the same probability of being detected. Here, $\mu_{\max}^{(i_2)} = \mu_{e1}^{(i_2)}$ for colluder $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_c^{(i_3)}$ for colluder $i_3 \in SC^{\text{all}}$. For any colluder $i \in SC$, $\mu_{\max}^{(i)}$ reaches its minimum value of 2.0545 when $\beta_1 = 0.4594$, $\beta_2 = 0.0951$, and $\alpha_1 = 0.2297$.

- Following (36), colluders can also achieve fairness of collusion by selecting

$$\beta_1 = \frac{4K^b}{\sqrt{2}K - (\sqrt{2}-1)K^b + (2-\sqrt{2})K^{\text{all}}} = 0.4594$$

$$\alpha_1 \geq \max\left\{\frac{3\sqrt{2}K^{b,e1} + 3K^b - 2K^{\text{all}}}{\sqrt{2}K - (\sqrt{2}-1)K^b + (2-\sqrt{2})K^{\text{all}}}, \frac{4(\sqrt{2}-1)K^{b,e1}}{\sqrt{2}K - (\sqrt{2}-1)K^b + (2-\sqrt{2})K^{\text{all}}}\right\} = 0.2297$$

$$\alpha_1 \leq \frac{4K^{b,e1}}{\sqrt{2}K - (\sqrt{2}-1)K^b + (2-\sqrt{2})K^{\text{all}}} = 0.0951, \text{ and}$$

$$\beta_2 = \frac{4\sqrt{2}K^{b,e1}}{\sqrt{2}K - (\sqrt{2}-1)K^b + (2-\sqrt{2})K^{\text{all}}} - \alpha_1 = 0.3248 - \alpha_1 \tag{39}$$

  during collusion. In this scenario, $\mu_{\max}^{(i_2)} = \mu_c^{(i_2)}$ for colluder $i_2 \in SC^{b,e1}$ and $\mu_{\max}^{(i_3)} = \mu_c^{(i_3)}$ for colluder $i_3 \in SC^{\text{all}}$, and $\mu_{\max}^{(i)} = 2.0545$ for all colluders.

The means of the detection statistics in these three scenarios are the same; therefore, colluders can choose either (37), (38) or (39) during collusion. [In fact, (37) and (38) are the two boundaries of (39).]

In the example of $(K^b, K^{b,e1}, K^{\text{all}}) = (50, 75, 125)$, the constraints (27) in Scenario 2 and (29) in Scenario 3 are satisfied, and the minimum value of $\mu_{\max}^{(i)}$ equals to 2.5298, when colluders select ($\beta_1 = 0.5657$, $\beta_2 = 0.0544$, $\alpha_1 = 0.4485$) or use ($\beta_1 = 0.5657$, $\beta_2 = 0.3929$, $\alpha_1 = 0.4071$) during collusion.

If $(K^b, K^{b,e1}, K^{\text{all}}) = (50, 125, 75)$, none of the six constraints in Section IV-D are satisfied, and colluders cannot generate a high-resolution colluded copy while still achieving fairness of the attack. They have to lower the resolution of the attacked copy to medium to guarantee the equal risk of all colluders.

## V. Simulation Results

In our simulations, we test over the first 40 frames of "carphone," and use $F_b = \{1, 5, \cdots, 37\}$, $F_{e1} = \{3, 7, \cdots, 39\}$ and

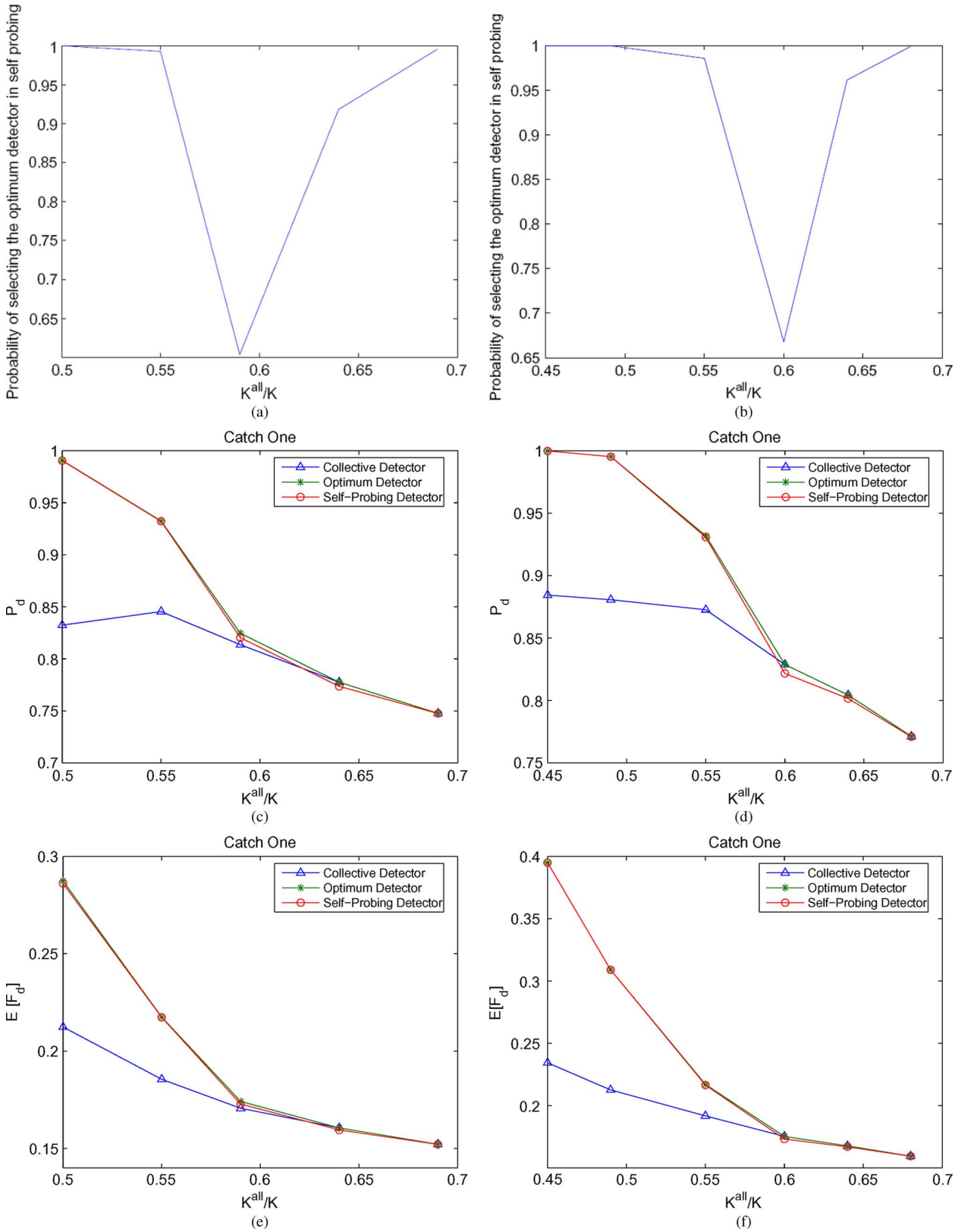



Fig. 7. Simulation results on the first 40 frames of sequence "carphone" from 10000 simulation runs. (a) and (b): Probability that the self-probing detector selects the optimum detection statistics with the largest mean. (c) and (d): $P_d$ when $P_{fp} = 10^{-3}$. (e) and (f): $E[F_d]$ with $E[F_{fp}]$ fixed as $10^{-3}$. In (a), (c), and (e), $R^b = 0.2$ and each point on the $x$ axis corresponds to a unique triplet $(K^b, K^{b,e1}, K^{\text{all}})$ where $K^b = 50$ and $K^{b,e1} = K - K^b - K^{\text{all}}$. In (b), (d), and (f), $R^b = 0.25$, and each point corresponds to a unique triplet $(K^b, K^{b,e1}, K^{\text{all}})$ where $K^b = 73$, and $K^{b,e1} = K - K^b - K^{\text{all}}$.

$F_{e2} = \{2, 4, \cdots, 40\}$ as an example of the temporal scalability. The lengths of the fingerprints embedded in the base layer, enhancement layer 1 and enhancement layer 2 are $N_b = 42987$, $N_{e1} = 42951$ and $N_{e2} = 85670$, respectively. We assume that there are a total of $M = 750$ users and $|\mathbf{U}^b| = |\mathbf{U}^{b,e1}| = |\mathbf{U}^{\text{all}}| = 250$. We first generate independent vectors following

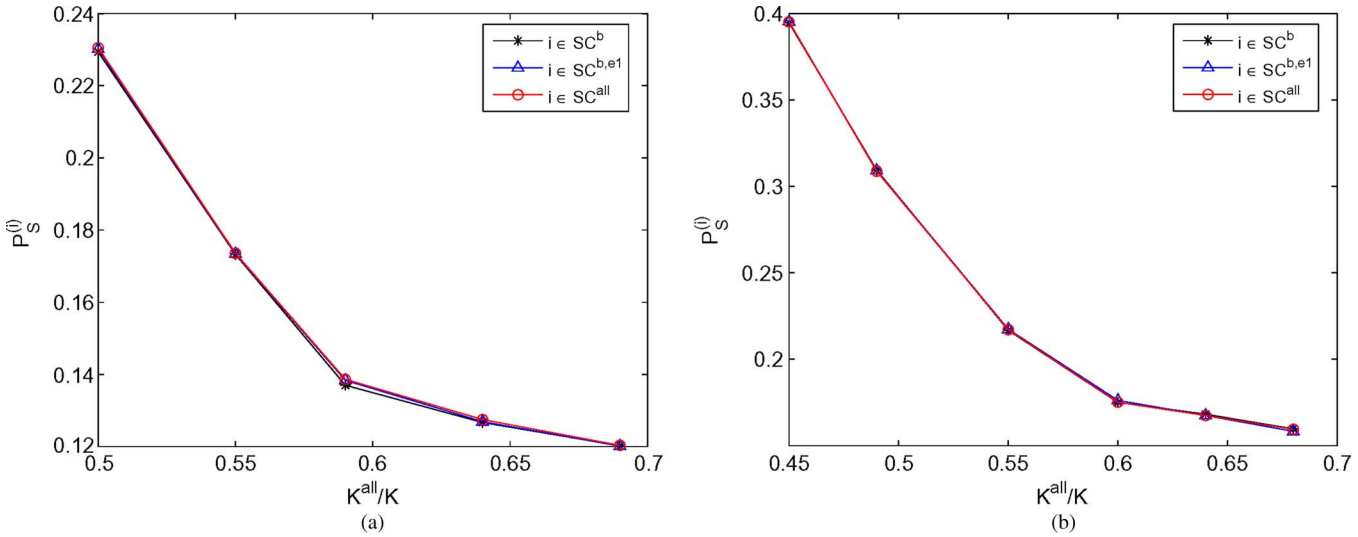



Fig. 8. Each colluder's probability of being detected ($P_s^{(i)}$) when they follow Section IV to select the collusion parameters. The simulation setup is similar to that in Fig. 7. There are a total of $K = 250$ colluders. In (a), $K^b = 50$ of them receive the fingerprinted based layer only, and each point on the $x$ axis corresponds to a unique triplet $(K^b, K^{b,e1}, K^{\text{all}})$ where $K^b = 50$ and $K^{b,e1} = K - K^b - K^{\text{all}}$. In (b), $K^b = 75$. Results are based 10 000 simulation runs. (a) $R^b = 0.20$. (b) $R^b = 0.25$.

Gaussian distribution $\mathcal{N}(0, 1/9)$, and then apply Gram-Schmidt orthogonalization to generate orthogonal fingerprints for different users.

We assume that $0 \leq K^b, K^{b,e1}, K^{\text{all}} \leq 250$ are the number of colluders in subgroups $SC^b$, $SC^{b,e1}$ and $SC^{\text{all}}$, respectively, and the total number of colluders is fixed to 250. During collusion, the colluders apply the intragroup collusion followed by the intergroup collusion, and follow Section IV when choosing the collusion parameters. In our simulations, we adjust the power of the additive noise such that $\|\mathbf{n}_j\|^2 = \|JND_j\mathbf{W}_j^{(i)}\|^2$ for every frame $j$ in the video sequence.

The fingerprint detector follows Section III-C when identifying selfish colluders. The detector first estimates the means of different detection statistics, selects the detection statistics with the largest estimated mean, and then identifies the colluders.

In Fig. 7, we compare the performance of three detectors: the simple collective detector in (4), the optimum detector which always selects the detection statistics with the largest mean, and the self-probing detector in Section III-C. Similar to Fig. 3, when the means of different detection statistics differ significantly from each other, the proposed self-probing detector in Section III-C always selects the optimum detection statistics with the largest mean. When the difference between different means is small, the optimum and the suboptimum detection statistics have approximately the same performance. Thus, even though the proposed method may make errors when deciding which detection statistics give the best performance, selecting the suboptimum detection strategy does not significantly deteriorate the detection performance when compared with the optimum detection statistics. In Fig. 7, the performance gap is smaller than $2 \times 10^{-3}$ and can be ignored. Exploring side information about collusion can significantly help improve the detection performance, and the proposed self-probing detector has approximately the same performance as the optimum detector with perfect knowledge of the detection statistics' means. Such result is a supportive evidence that the self-probing algorithm can correctly estimate the mean value of the detection statistics an help choose the detector with best performance. It is clear from Fig. 7 that the probability of catching at least one colluder has been improved by 17% when $R^{\text{all}} = 0.5$, $R^b = 0.2$, 12% when $R^{\text{all}} = 0.45$, $R^b = 0.25$ and the improved probabilities are closed to 1 in both cases.

Fig. 8 plots each colluder's probability of being detected when they follow Section IV to select the collusion parameters. It is obvious that in this example, all colluders have the same probability of being detected and this multiuser collusion achieves fairness of the attack.

In order to show that the self-probing detector can be applied to various types of videos, we also run the simulation on "tennis," which is a fast-motion video. We use the first 28 frames of "tennis," and use $F_b = \{1, 5, \cdots, 37\}$, $F_{e1} = \{3, 7, \cdots, 39\}$, and $F_{e2} = \{2, 4, \cdots, 40\}$ as an example of the temporal scalability. The lengths of the fingerprints embedded in the base layer, enhancement layer 1 and enhancement layer 2 are $N_b = 45092$, $N_{e1} = 45103$ and $N_{e2} = 90174$, respectively. Other settings are the same as above. Fig. 9 shows $E[P_d]$ and $P_d$ of the optimal detector, self-probing detector and the collective detector when $R^b = 0.25$. It is clear from Fig. 9 that the proposed self-probing detector also achieves almost the same performance as the optimal detector which has perfect information about the mean value. Such result shows that the detection performance of the self-probing detector is not influenced by the video characteristics.

## VI. Conclusion

This paper studies user behavior in the multimedia fingerprint social networks. We model the complex dynamics of the users in the social network using game theory and find the optimal strategies of both players in the game. We study how side information about collusion can help the fingerprint detector increase the traitor-tracing capability, and influence the strategies of the colluders and the forensic detector.

We first investigated multimedia forensics with side information. Our analysis and simulation results show that the side in-

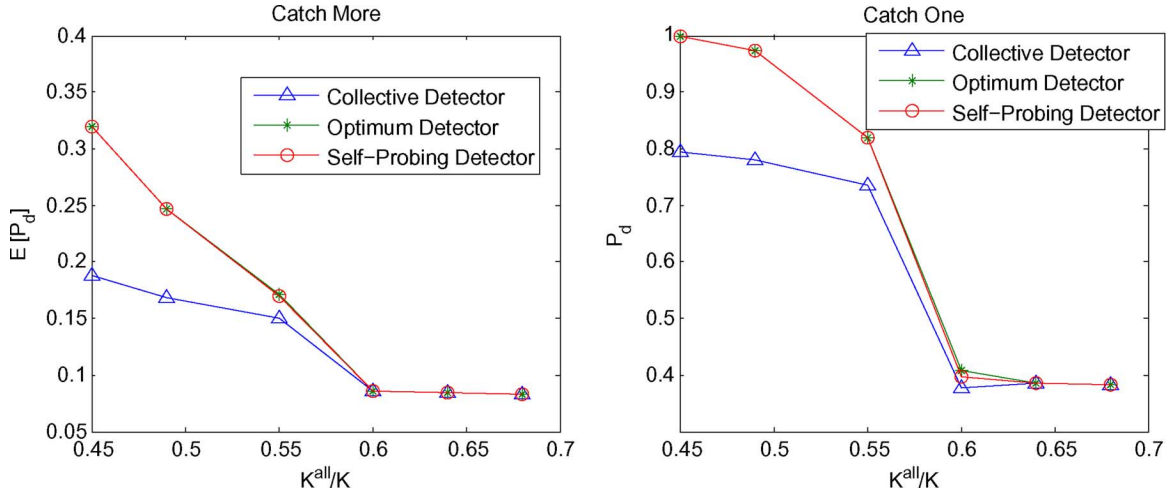



Fig. 9. Simulation results on first 28 frames of "tennis" from 1000 simulation runs. $E[F_d]$ with $E[F_{fp}]$ fixed as $10^{-3}$ and $P_d$ when $P_{fp} = 10^{-3}$.

formation about the means of the detection statistics can help the detector significantly improve the collusion resistance. We then propose a method for the detector himself/herself to probe such side information from the colluded copy. Our simulation results demonstrate that the proposed self-probing detector has approximately the same performance as the optimal fingerprint detector, and the difference between these two can be ignored.

Side information not only improves the fingerprint detector's collusion resistance, but it also affects each colluder's probability of being detected and makes some colluders take a larger risk than others. Thus, it breaks the collective fairness equilibrium between the colluders and the fingerprint detector, and they have to choose different strategies. We model the colluder-detector dynamics with side information as a zero-sum game. We show that under the assumption that colluders demand absolute fairness of the attack, the min-max solution achieves the equilibrium which is the optimal strategy of all users in the multimedia fingerprint social network. Neither the colluders nor the fingerprint detector can further increase their payoff and, therefore, they have no incentive to move away from this equilibrium.

## APPENDIX
## PROOF OF (16), (17), (18), AND FEASIBLE SETS

### A. Proof of (16)

If $\mu_{\max}^{(i)} = \mu_b^{(i)}$, then $\mu_b^{(i)} \geq \mu_{e1}^{(i)}$ and $\mu_b^{(i)} \geq \mu_c^{(i)}$. Thus, from (15)

$$\mu_b^{(i)} \geq \mu_{e1}^{(i)} \Leftrightarrow \frac{\beta_2\sqrt{N_b}}{K^{b,e1}}\sigma_W \geq \frac{\alpha_1\sqrt{N_{e1}}}{K^{b,e1}}\sigma_W \Leftrightarrow \beta_2 \geq \frac{\alpha_1\sqrt{N_{e1}}}{\sqrt{N_b}}. \quad (40)$$

Similarly, we have

$$\mu_b^{(i)} \geq \mu_c^{(i)} \Leftrightarrow \frac{\beta_2\sqrt{N_b}}{K^{b,e1}}\sigma_W \geq \frac{\beta_2 N_b + \alpha_1 N_{e1}}{K^{b,e1}\sqrt{N_b+N_{e1}}}\sigma_W \Leftrightarrow \beta_2 \geq \frac{\alpha_1 N_{e1}}{\sqrt{N_b}(\sqrt{N_b+N_{e1}}-\sqrt{N_b})}. \quad (41)$$

Note that $\sqrt{N_b}+\sqrt{N_{e1}} \geq \sqrt{N_b+N_{e1}}$. Thus, $\sqrt{N_{e1}} \geq \sqrt{N_b+N_{e1}}-\sqrt{N_b}$ and $\alpha_1 N_{e1}/\sqrt{N_b}(\sqrt{N_b+N_{e1}}-\sqrt{N_b}) \geq \alpha_1\sqrt{N_{e1}}/\sqrt{N_b}$. Therefore, combining (40) and (41), for colluder $i \in SC^{b,e1}$

$$\mu_{\max}^{(i)} = \mu_b^{(i)} \quad \text{if and only if} \quad \beta_2 \geq \frac{\alpha_1 N_{e1}}{\sqrt{N_b}(\sqrt{N_b+N_{e1}}-\sqrt{N_b})}. \quad (42)$$

### B. Proof of (17)

If $\mu_{\max}^{(i)} = \mu_{e1}^{(i)}$, $\mu_{e1}^{(i)} \geq \mu_b^{(i)}$ and $\mu_{e1}^{(i)} \geq \mu_c^{(i)}$. Thus,

$$\mu_{e1}^{(i)} \geq \mu_b^{(i)} \Leftrightarrow \frac{\alpha_1\sqrt{N_{e1}}}{K^{b,e1}}\sigma_W \geq \frac{\beta_2\sqrt{N_b}}{K^{b,e1}}\sigma_W \Leftrightarrow \beta_2 \leq \frac{\alpha_1\sqrt{N_{e1}}}{\sqrt{N_b}}$$

and

$$\mu_{e1}^{(i)} \geq \mu_c^{(i)} \Leftrightarrow \frac{\alpha_1\sqrt{N_{e1}}}{K^{b,e1}}\sigma_W \geq \frac{\beta_2 N_b + \alpha_1 N_{e1}}{K^{b,e1}\sqrt{N_b+N_{e1}}}\sigma_W \Leftrightarrow \beta_2 \leq \frac{\alpha_1\sqrt{N_{e1}}(\sqrt{N_b+N_{e1}}-\sqrt{N_{e1}})}{N_b}. \quad (43)$$

It is straightforward to show that $\sqrt{N_b+N_{e1}}-\sqrt{N_{e1}} \leq \sqrt{N_b}$ and $\alpha_1\sqrt{N_{e1}}(\sqrt{N_b+N_{e1}}-\sqrt{N_{e1}})/N_b \geq \alpha_1\sqrt{N_{e1}}/\sqrt{N_b}$. Thus, combining the results in (43), we have

$$\mu_{\max}^{(i)} = \mu_{e1}^{(i)} \quad \text{if and only if} \quad \beta_2 \leq \frac{\alpha_1\sqrt{N_{e1}}\left(\sqrt{(N_b+N_{e1})}-\sqrt{N_{e1}}\right)}{N_b}. \quad (44)$$

### C. Proof of (18)

When $\mu_{\max}^{(i)} = \mu_c^{(i)}$, $\mu_c^{(i)} \geq \mu_b^{(i)}$, and $\mu_c^{(i)} \geq \mu_{e1}^{i)}$. Following the same analysis as in the previous two scenarios

$$\mu_c^{(i)} \geq \mu_b^{(i)} \Leftrightarrow \beta_2 \leq \frac{\alpha_1 N_{e1}}{\sqrt{N_b}(\sqrt{N_b+N_{e1}}-\sqrt{N_b})}$$

and

$$\mu_c^{(i)} \geq \mu_{e1}^{(i)} \Leftrightarrow \beta_2 \geq \frac{\alpha_1\sqrt{N_{e1}}(\sqrt{N_b+N_{e1}}-\sqrt{N_{e1}})}{N_b}. \quad (45)$$

Note that $\sqrt{N_b+N_{e1}} \leq \sqrt{N_b}+\sqrt{N_{e1}}$. Therefore, we have

$$\sqrt{N_b+N_{e1}}-\sqrt{N_b} \leq \sqrt{N_{e1}}$$

and

$$\begin{aligned} & \sqrt{N_b+N_{e1}}-\sqrt{N_{e1}} \le \sqrt{N_b} \\ \Leftrightarrow \quad & \frac{\sqrt{N_b+N_{e1}}-\sqrt{N_{e1}}}{\sqrt{N_b}} \le \frac{\sqrt{N_{e1}}}{\sqrt{N_b+N_{e1}}-\sqrt{N_b}} \\ \Leftrightarrow \quad & \frac{\alpha_1\sqrt{N_{e1}}(\sqrt{N_b+N_{e1}}-\sqrt{N_{e1}})}{N_b} \\ & \le \frac{\alpha_1 N_{e1}}{\sqrt{N_b}(\sqrt{N_b+N_{e1}}-\sqrt{N_b})}. \end{aligned} \tag{46}$$

Consequently, $\mu_{\max}^{(i)} = \mu_c^{(i)}$ if and only if

$$\frac{\alpha_1\sqrt{N_{e1}}\left(\sqrt{(N_b+N_{e1})}-\sqrt{N_{e1}}\right)}{N_b} \le \beta_2 \le \frac{\alpha_1 N_{e1}}{\sqrt{N_b}(\sqrt{N_b+N_{e1}}-\sqrt{N_b})}. \tag{47}$$

## REFERENCES


[1] H. Zhao, W. S. Lin, and K. J. R. Liu, "Behavior modeling and forensics for multimedia social networks: A case study in multimedia fingerprinting," *IEEE Signal Process. Mag.*, vol. 26, no. 1, pp. 118–139, Jan. 2009.

[2] I. Cox, M. Miller, and J. Bloom, *Digital Watermarking*. San Mateo, CA: Morgan Kaufmann , 2001.

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

[4] I. Cox and J. P. Linnartz, "Some general methods for tampering with watermaking," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 587–593, May 1998.

[5] K. J. R. Liu, W. Trappe, Z. J. Wang, M. Wu, and H. Zhao, "Multimeida fingerprinting forensics for traitor tracing," in *EURASIP Book Series on Signal Processing and Communications*. New York: Hindawi, 2005.

[6] G. Doerr, J. L. Dugelay, and L. Grange, "Exploiting self-similarities to defeat digital watermarking systems: A case study on still images," in *Proc. 2004 ACM Multimedia and Security Workshop*, 2004.

[7] D. Kiroski and F. A. P. Petitcolas, "Blind pattern matching attack on watermarking systems," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 1045–1053, 2003.

[8] Z. J. Wang, M. Wu, H. Zhao, W. Trappe, and K. J. R. Liu, "Anti-collusion forensics of multimedia fingerprinting using orthogonal modulation," *IEEE Trans. Image Process.*, vol. 14, no. 6, pp. 804–821, Jun. 2005.

[9] H. Zhao, M. Wu, Z. J. Wang, and K. J. R. Liu, "Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting," *IEEE Trans. Image Process.*, vol. 14, no. 5, pp. 646–661, May 2005.

[10] H. V. Zhao and K. J. R. Liu, "Traitor-within-traitor behavior forensics: Strategy and risk minimization," *IEEE Trans. Inf. Forensic Security*, vol. 1, no. 4, pp. 440–456, Dec. 2006.

[11] F. Zane, "Efficient watermark detection and collusion security," *Proc. Financial Cryptogr., Lecture of Notes in Comput. Sci.*, vol. 1962, pp. 21–32, Feb. 2000.

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

[13] Z. J. Wang, M. Wu, W. Trappe, and K. J. R. Liu, "Group-oriented fingerprinting for multimedia forensics," *EURASIP J. Appl. Signal Process., Special Issue on Multimedia Security and Rights Manage.*, vol. 2004, no. 14, pp. 2142–2162, Nov. 2004.

[14] S. He and M. Wu, "Joint coding and embedding techniques for multimedia fingerprinting," *IEEE Trans. Inf. Forensic Security*, vol. 1, no. 2, pp. 231–247, Jun. 2006.

[15] H. Zhao and K. J. R. Liu, "Behavior forensics for scalable multiuser collusion: Fairness and effectiveness," *IEEE Tran. Inf. Forensic Security*, vol. 1, no. 3, pp. 311–329, Sep. 2006.

[16] Y. Wang, J. Ostermann, and Y. Zhang, *Video Processing and Communications*, 1st ed. Englewood Cliffs, NJ: Prentice-Hall, 2001.

[17] C. Podilchuk and W. Zeng, "Image adaptive watermarking using visual models," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 525–540, May 1998.

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

[19] H. V. Poor, *An Introduction to Signal Detection and Estimation*, 2nd ed. New York: Springer-Verlag, 1999.

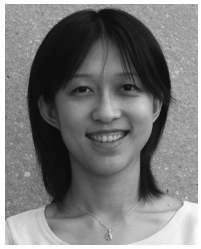
[20] W. S. Lin, H. V. Zhao, and K. J. R. Liu, "A game theoretic framework for colluder-detector behavior forensics," in *IEEE Int. Conf. Acoust., Speech Signal Process.*, May 2007.

[21] G. Owen, *Game Theory*, 3rd ed. New York: Academic, 2007.

[22] D. Fudenberg and J. Tirole, *Game Theory*. Cambridge, U.K.: MIT Press, 1991.


**W. Sabrina Lin** (M'06) received the B.S. and M.S. degrees from National Taiwan University, in 2002 and 2004, respectively, and the Ph.D. degree from the University of Maryland, College Park, in 2008, all in electrical engineering.

Her research interests are in the area of information security and forensics, multimedia signal processing, and multimedia social network analysis. She received the University of Maryland Future Faculty Fellowship in 2007.



**H. Vicky Zhao** (M'05) received the B.S. and M.S. degrees from Tsinghua University, China, in 1997 and 1999, respectively, and the Ph.D. degree from the University of Maryland, College Park, in 2004, all in electrical engineering.

She was a Research Associate with the Department of Electrical and Computer Engineering and the Institute for Systems Research, University of Maryland, College Park, from January 2005 to July 2006. Since August 2006, she has been an Assistant Professor with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, Canada. Her research interests include information security and forensics, multimedia, digital communications, and signal processing. She coauthored the book "*Multimedia Fingerprinting Forensics for Traitor Tracing*" (New York: Hindawi, 2005).

Dr. Zhao received the IEEE Signal Processing Society (SPS) 2008 Young Author Best Paper Award. She is the Associate Editor for IEEE SIGNAL PROCESSING LETTERS and *Journal of Visual Communication and Image Representation*.

**K. J. Ray Liu** (F'03) is a Distinguished Scholar-Teacher of University of Maryland, College Park. He is Associate Chair, Graduate Studies and Research, Electrical and Computer Engineering Department, and leads the Maryland Signals and Information Group conducting research encompassing broad aspects of information science and technology including communications and networking, information forensics and security, multimedia signal processing, and biomedical engineering.

Dr. Liu is the recipient of numerous honors and awards, including best paper awards from the IEEE Signal Processing Society, the IEEE Vehicular Technology Society, and EURASIP; an IEEE Signal Processing Society Distinguished Lecturer, the EURASIP Meritorious Service Award, and the National Science Foundation Young Investigator Award. He also received various teaching and research recognitions from University of Maryland, including the university-level Invention of the Year Award; and Poole and Kent Senior Faculty Teaching Award and Outstanding Faculty Research Award, both from A. James Clark School of Engineering. He is a Fellow of AAAS. He was Vice President–Publications of the IEEE Signal Processing Society. He was the Editor-in-Chief of the *IEEE Signal Processing Magazine* and the founding Editor-in-Chief of the *EURASIP Journal on Applied Signal Processing*. His recent books include *Cooperative Communications and Networking* (Cambridge Univ. Press, 2008); *Resource Allocation for Wireless Networks: Basics, Techniques, and Applications* (Cambridge Univ. Press, 2008); *Ultra-Wideband Communication Systems: The Multiband OFDM Approach* (IEEE-Wiley, 2007); *Network-Aware Security for Group Communications* (Springer, 2007); *Multimedia Fingerprinting Forensics for Traitor Tracing* (Hindawi, 2005); *Handbook on Array Processing and Sensor Networks* (IEEE-Wiley, 2009).