Cooperation and Coalition in Multimedia Fingerprinting Colluder Social Networks

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

***Abstract*—Users in multimedia social networks actively interact with each other. It is crucial to study the complex user dynamics and analyze its impact on the performance of multimedia social networks. This paper uses multimedia fingerprinting as an example and studies user dynamics in colluder social networks. During collusion, a group of attackers collectively attack multimedia fingerprinting system and use multimedia content illegally. This paper analyzes the incentives of cooperation among attackers and investigates how colluders form their coalitions to maximize their payoffs. We present a game-theoretic framework to model the complex dynamics among colluders, analyze when attackers cooperate with each other, and investigate how a colluder selects his/her fellow attackers to maximize his/her own payoff. We analyze multiuser collusion in two scenarios: when all attackers receive fingerprinted copies of the same resolution, and when they have copies of different resolutions. The proposed framework considers both the colluders' risk of being detected by the digital rights enforcer and the reward received from illegal usage of multimedia content. Our analysis shows that in both scenarios, colluding with more attackers does not always increase an attacker's utility, and attackers may not always want to cooperate with each other. We first examine the necessary conditions for attackers to collude together, and study how they select the collusion parameters such that cooperation benefits all colluders. We then study how the number of colluders affects each attacker's utility, and investigate the optimum strategy that an attacker should use to select fellow attackers and to form a coalition in order to maximize his or her own payoff.**

***Index Terms*—Coalition formation, game theory, multiuser collusion, multimedia fingerprinting.**

I. Introduction

In THE PAST decade, we witness the emergence of large-scale media-sharing social networks such as Napster, Flickr, YouTube, CoolStreaming, and PPLive, where millions of users form a dynamically changing infrastructure to share multimedia contents [1]–[5]. Social networks are defined as "social structures that can be represented as *networks*—as sets of *nodes* (for social system members) and sets of *ties* depicting their interconnections [6]." Nodes in the network can be individual persons, small groups, or formal organizations, who are connected to each other via certain relationship, such as friendship, trade, or colleagues. In the above mentioned social networks, users are the nodes who are connected to each other via sharing of multimedia content and resources, e.g., upload bandwidth. In these social networks, users actively interact with each other, and such user dynamics not only influences each individual user but also affects the system performance. Therefore, it is of ample importance to analyze the impact of human factors on media-sharing social networks, and to provide important guidelines to better design of multimedia systems. The area of human and social dynamics has recently been identified by the U.S. National Science Foundation as one of its five priority areas, which also shows the importance of this emerging interdisciplinary research area.

This paper analyzes user dynamics in media-sharing social networks, where users cooperate with each other to share multimedia data. Cooperation enables users to access extra resources from others and thus receive higher payoffs. However, cooperation may also incur cost to users and cooperating with more users does not always increase a user's utility, as shown in prior works on cooperation in wireless networks [7] and cooperative spectrum sensing in cognitive radios [8]. In addition, it has been observed that in many social networks, nodes tend to create tightly knit groups where nodes are connected via many direct, reciprocated choice relations [9]. Analysis of these cliques is an important research area in social network analysis to identify such cohesive groups of nodes who share information, achieve homogeneity of thoughts and behavior, and act collectively, and to study when and how nodes form cliques/coalitions [9], [10]. This paper provides a case study of coalition formation in multiuser collusion against multimedia fingerprinting, and builds a game-theoretic framework to analyze when users cooperate with each other and how they select partners to maximize their own utilities.

Recent popularity of peer-to-peer and media-sharing networks has raised great concerns on copyright infringement in these networks, and it was reported in [11] that peer-to-peer traffic in pirate content may consume 49% to 89% of all Internet traffic during the day and up to 99% at night. Copyright industries are looking for novel technologies to throttle illegal file sharing and to protect intellectual property rights. Multimedia fingerprinting is an emerging technology that offers proactive post-delivery protection of multimedia content [12]–[16]. It labels each distributed copy with the corresponding user's identification information, called *fingerprint*, which can be used to track the distribution of multimedia data and to identify the source of illicit copies. Multiuser collusion is a cost-effec-

Manuscript received April 29, 2011; revised November 18, 2011; accepted March 08, 2012. Date of publication March 20, 2012; date of current version May 11, 2012. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Ton Kalker.

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

W. S. Lin is with Intel Corporation, Hillsboro, OR 97124 USA (e-mail: wylin1981@gmail.com).

K. J. Ray Liu is with the Department of Electrical and Computer Engineering, University of Maryland at College Park, College Park, MD 20742 USA (e-mail: kjrliu@umd.edu).

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/TMM.2012.2191394

TABLE I
LIST OF SYMBOLS USED IN THIS PAPER

Set of frame indices encoded in base layer	F_b	Set of frame indices encoded in enhancement layer	F_e
Set of frame indices of user $u^{(i)}$'s copy	$F^{(i)}$	Normalized temporal resolution of $u^{(i)}$ ($\|F^{(i)}\|/(\|F_b\|+\|F_e\|)$	$f^{(i)}$
Normalized temporal resolution of a low-resolution copy ($\|F_b\|/(\|F_b\|+\|F_e\|)$	f_b	Lengths of the fingerprints embedded in the base layer	N_b
Lengths of the fingerprints embedded in the enhancement layer	N_e	Set of colluders who receive a low resolution copy	SC^b
Set of colluders who receive a high resolution copy	SC^{be}	Total number of colluders ($K^b + K^{be}$)	K
Set of frame indices of the colluded copy	F_c	Normalized resolution of the colluded copy	f_c

tive attack against multimedia fingerprinting, where a group of attackers work collectively to remove or attenuate the embedded fingerprints. Note that colluders form a social network; colluders are the nodes who are connected to each other by sharing their fingerprinted copies, the risk of being detected, and the reward from illegal usage of multimedia content. During collusion, attackers negotiate with each other on fair distribution of the risk and the reward. Most prior works considered the equal-risk fairness criterion where all colluders have the same probability of being detected [17]–[20]. In [21], we studied different fairness constraints in multiuser collusion, and investigated how colluders with conflicting objectives bargain with each other to reach an agreement on the fair allocation of risk and reward. Based on the above analysis of collusion attacks, our prior work in [22] investigated techniques for the fingerprint detector to probe side information about collusion from the colluded copy, and to select the optimum detection strategy that maximizes the detection probability.

However, these prior works do not answer the questions *when* attackers would collaborate with each other and *how* to form a coalition. An attacker first needs to decide whether to participate in collusion and with whom to collude. When colluders' goal is to minimize their probability of being detected, the analysis in [16] and [17] showed that with orthogonal fingerprinting, a collusion attack with more attackers reduces the energy of each contributing fingerprint by a larger ratio and, therefore, each attacker has a smaller chance of being caught. Thus, to minimize the risk, colluders are always willing to cooperate with each other, and a colluder should find as many fellow attackers as possible.

Nevertheless, colluding with more attackers also means sharing with more people the reward from illegal usage of multimedia and, therefore, colluders may not always want to cooperate. Furthermore, a colluder also needs to decide with whom to collude, which has not been addressed in the literature. We use game theory to analyze these complex dynamics among colluders and take into consideration both the risk and the reward of collusion. In this paper, we use orthogonal fingerprint modulation and linear averaging collusion as an example, and provide a case study of coalition formation in colluder social networks. For other fingerprinting and collusion models, the same procedure and techniques can be used to analyze colluder behavior. In this work, we consider two scenarios: when all attackers receive fingerprinted copies of the same resolution and when they receive copies of different resolutions. We investigate under what conditions colluders will cooperate with each other, study how they choose the collusion parameters to ensure that all colluders can improve their payoffs, and analyze how colluders form a coalition to maximize his or her own payoff. Such analysis helps us have a better understanding of multiuser collusion, and offers important guidelines to better design of collusion-resistant multimedia fingerprinting systems.

The rest of this paper is organized as follows. Section II describes our system model and Section III introduces the game-theoretic framework that we use to model the complex dynamics among colluders. Section IV and Section V analyze the dynamics among colluders when they receive copies of the same resolution and when the fingerprinted copies have different resolutions, respectively. Section VI shows the simulation results, and conclusions are drawn in Section VII. Some of the symbols used in the following sections are summarized in Table I.

II. MULTIMEDIA FINGERPRINTING WITH SCALABLE VIDEO CODING

A. Multimedia Fingerprinting

To address network and device heterogeneity, scalable video coding decomposes a video sequence into layers of different priority. The base layer contains the most important information of the video and is received by all users, and the enhancement layers gradually refine the reconstructed sequence at the decoder's side and are only received by users with sufficient bandwidth. Using two-layer temporal scalability as an example, we use frame skipping and frame copying to implement temporal decimation and interpolation, respectively [23]. For example, the base layer encodes the odd frames, and the enhancement layer encodes the difference between the even and the odd frames.

Let F_b and F_e be the sets with indices of frames encoded in the base layer and the enhancement layer, respectively. The set $F^{(i)}$ contains the indices of all frames that user $u^{(i)}$ receives. If $u^{(i)}$ receives a low-resolution copy, then $F^{(i)} = F_b$ and the normalized frame rate of $u^{(i)}$'s copy is $f^{(i)} = f_b \triangleq |F_b|/(|F_b|+|F_e|) < 1$. The normalized frame rate $f^{(i)} = 1$ if $u^{(i)}$ receives both layers from the content owner.

With scalable video coding, a multimedia fingerprinting system consists of three parts: fingerprint embedding, multiuser collusion, and colluder identification [12].

1) Fingerprint Embedding: In this paper, we consider spread spectrum embedding that has been widely used in multimedia fingerprinting due to its robustness against many single-copy attacks [24]. For the jth frame in the video sequence represented by a vector $\mathbf{S}_j$ of length N, and for each user $u^{(i)}$ who subscribes to frame j, the content owner generates a unique fingerprint $\mathbf{W}_j^{(i)}$ of length N. The fingerprinted frame j that will be distributed to $u^{(i)}$ is $\mathbf{X}_j^{(i)} = \mathbf{S}_j + JND_j \cdot \mathbf{W}_j^{(i)}$. The term JND_j

is the *just-noticeable-difference* from human visual models [24], and it is used to control the energy of the embedded fingerprints. Finally, the content owner transmits to user $u^{(i)}$ all the fingerprinted frames $\{\mathbf{X}_j^{(i)}\}$ that $u^{(i)}$ subscribes to.

We assume that the total number of users is much smaller than the length of the embedded fingerprints and consider orthogonal fingerprint modulation [16], where fingerprints assigned to different users are orthogonal to each other and have equal energies.

2) Multiuser Collusion: We consider the scenario where colluders wish to generate a high-resolution colluded copy whenever possible and the normalized frame rate of the colluded copy f_c is 1 when at least one attacker receives both layers. In addition, we consider the simple scenario where colluders who receive fingerprinted copies of the same resolution agree to share the same risk and receive the same reward.

When all attackers receive copies of the same resolution, a simple average of all copies attenuates the energy of all contributing fingerprints and, therefore, reduces the colluders' probability of being detected [17]. When attackers receive copies of different resolutions, they apply the two-stage collusion in [20] as follows. First, colluders divide themselves into two non-overlapping subgroups: SC^b with all colluders who receive the base layer only, and SC^{be} with all colluders who receive a high-resolution copy. Let K^b be the number of colluders in SC^b and K^{be} be the number of colluders in SC^{be}. Then, they apply the *intragroup collusion attack*. For each frame $j \in F_b$ in the base layer, colluders in SC^b average all fingerprinted copies that they have and generate $\mathbf{Z}_j^b = \sum_{k\in SC^b} \mathbf{X}_j^{(k)}/K^b$, and similarly, for every frame $j \in F_b \cup F_e$ in the video sequence, colluders in SC^{be} generate $\mathbf{Z}_j^{be} = \sum_{k\in SC^{be}} \mathbf{X}_j^{(k)}/K^{be}$. This ensures that all colluders who receive copies of the same resolution have the same probability of being detected. Finally, colluders apply the *intergroup collusion* to generate the final colluded copy $\mathbf{V}$. For each frame $j \in F_b$ in the base layer, $\mathbf{V}_j = \beta\mathbf{Z}_j^b + (1-\beta)\mathbf{Z}_j^{be} + \mathbf{n}_j$, where $0 \le \beta \le 1$, and for each frame $l \in F_e$ in the enhancement layer, $\mathbf{V}_l = \mathbf{Z}_l^{be} + \mathbf{n}_l$. The additive noise $\mathbf{n}_l$ is used to further hinder fingerprint detection. Colluders select the parameter β to achieve "*fair*" distribution of the risk among colluders in different subgroups.

3) Colluder Identification: Once the content owner discovers the existence of an illegal copy of multimedia, the detector first extracts the fingerprint $\mathbf{Y}_j = (\mathbf{V}_j - \mathbf{S}_j)/JND_j$ from the jth frame of the test copy $\mathbf{V}_j$. Then, for each user $u^{(i)}$, the detector calculates the correlation-based detection statistic $TN^{(i)} = \sum_j \langle \mathbf{Y}_j, \mathbf{W}_j^{(i)}\rangle / \sqrt{\sum_j \|\mathbf{W}_j^{(i)}\|^2}$ to measure the similarity between the extracted fingerprint and the original fingerprint. Here, $\langle \mathbf{a}, \mathbf{b}\rangle$ is the inner product of two vectors $\mathbf{a}$ and $\mathbf{b}$, $\|\mathbf{a}\|$ is the l_2 norm of the vector $\mathbf{a}$, and the summations are over all frames that user $u^{(i)}$ subscribes to. Finally, the detector compares the detection statistics with a predetermined threshold h, and outputs the estimated identities of the colluders $\widehat{SC} = \{i : TN^{(i)} > h\}$.

B. Colluder Identification Using Self-Probing Detector

In the two-layer scalable multimedia fingerprinting system in Section II-A, for user $u^{(i)}$ who receives a high resolution fingerprinted copy, let $\mathbf{W}_b^{(i)}$ and $\mathbf{W}_e^{(i)}$ denote $u^{(i)}$'s fingerprints that are embedded in the base layer and the enhancement layer, respectively. Let $\mathbf{Y}_b$ and $\mathbf{Y}_e$ be the fingerprints extracted from the base layer and the enhancement layer of the test copy, respectively.

In such a system, there are many different ways to determine if $u^{(i)}$ participates in collusion. For example, the fingerprint detector can use $\mathbf{Y}_b$ and $\mathbf{Y}_e$ collectively to determine whether $u^{(i)}$ is a colluder, and the fingerprint detector uses the collective detection statistic

$$TN_c^{(i)} = \frac{\left\langle \mathbf{Y}_b, \mathbf{W}_b^{(i)} \right\rangle + \left\langle \mathbf{Y}_e, \mathbf{W}_e^{(i)} \right\rangle}{\sqrt{\left\|\mathbf{W}_b^{(i)}\right\|^2 + \left\|\mathbf{W}_e^{(i)}\right\|^2}} \tag{1}$$

to measure the similarity between the extracted and the original fingerprints. From [22], with orthogonal fingerprint modulation, if the detection noise $\mathbf{d}_j = \mathbf{n}_j/JND_j$ is i.i.d. Gaussian $\mathcal{N}(0, \sigma_n^2)$, then $TN_c^{(i)}$ follows the Gaussian distribution

$$TN_c^{(i)} \sim \begin{cases} \mathcal{N}\left(\mu_c^{be} = \frac{(1-\beta)N_b + N_e}{K^{be}\sqrt{N_b+N_e}}\sigma_w, \sigma_n^2\right), & \text{if } i \in SC^{be} \\ \mathcal{N}\left(0, \sigma_n^2\right), & \text{if } i \notin SC^{be}. \end{cases} \tag{2}$$

In (2), N_b and N_e are the lengths of the fingerprints embedded in the base layer and the enhancement layer, respectively, and σ_w^2 is the variance of the fingerprint $\mathbf{W}^{(i)}$.

The fingerprint detector can also use the fingerprint extracted from each individual layer to determine whether $u^{(i)}$ participates in collusion, and uses

$$TN_t^{(i)} = \frac{\left\langle \mathbf{Y}_t, \mathbf{W}_t^{(i)} \right\rangle}{\left\|\mathbf{W}_t^{(i)}\right\|} \sim \begin{cases} \mathcal{N}\left(\mu_t^{be}, \sigma_n^2\right), & \text{if } i \in SC^{be} \\ \mathcal{N}\left(0, \sigma_n^2\right), & \text{if } i \notin SC^{be} \end{cases} \tag{3}$$

to calculate the similarity between the extracted and the original fingerprints. Here, the subscript "t" is the layer index and is either "b" (the base layer) or "e" (the enhancement layer). In (3), $\mu_b^{be} = (1-\beta)\sqrt{N_b}\sigma_w/K^{be}$ and $\mu_e^{be} = \sqrt{N_e}\sigma_w/K^{be}$.

Comparing (2) and (3), $TN_c^{(i)}$, $TN_b^{(i)}$, and $TN_e^{(i)}$ have the same variance but different statistical means, and the one with the largest mean gives the best detection performance. When $\beta < \beta^+ \triangleq \sqrt{N_b+N_e}(\sqrt{N_b+N_e} - \sqrt{N_e})/N_b$, $\mu_c^{be} > \max\{\mu_b^{be}, \mu_e^{be}\}$. For a colluder in SC^{be} who contributes a high-resolution copy, the energy of his/her fingerprint is spread out in both layers in the colluded copy, and thus, it is better to use $TN_c^{(i)}$ and examine the entire video to achieve higher robustness against collusion attacks. If $\beta > \beta^+$, then $\mu_e^{be} > \max\{\mu_c^{be}, \mu_b^{be}\}$, and for a colluder $i \in SC^{be}$, the energy of his/her fingerprint in the base layer of the colluded copy is very small, as it is also averaged with the contributions from colluders in SC^b. Thus, it is better to examine the enhancement layer only to determine if user i participates in collusion and use $TN_e^{(i)}$ for better detection performance. The self-probing detector in [22] probes the statistical means of different detection statistics from the colluded copy, and adaptively changes the detection strategy to maximize the detection performance. From [22], the self-probing detector has approximately the same performance as the optimal detector, who has perfect

knowledge of the statistical means of different detection statistics and always chooses the one with better collusion resistance.

III. Utility Function and Feasible Collusion

The first step of understanding colluder dynamics is to define the utility function ν that each colluder wants to maximize. During collusion, colluders share the risk of being captured by the digital rights enforcer as well as the reward from illegal usage of multimedia content. For colluder $u^{(i)}$, let $P_d^{(i)}$ be his or her probability of being detected, $L^{(i)}$ be $u^{(i)}$'s loss if he or she is caught by the fingerprint detector, and $R^{(i)}$ be the reward that $u^{(i)}$ receives from collusion if he or she is not detected. The loss $L^{(i)}$ and the reward $R^{(i)}$ are nonnegative real numbers. A natural definition of the utility function is the expected payoff that $u^{(i)}$ receives by participating in collusion, that is

$$\nu^{(i)} = -P_d^{(i)} L^{(i)} + \left(1 - P_d^{(i)}\right) R^{(i)}. \tag{4}$$

We will analyze the three terms—$P_d^{(i)}$, $L^{(i)}$, and $R^{(i)}$—in detail in this section.

A. Probability of Being Detected $P_d^{(i)}$

We first consider the scenario where colluders receive fingerprinted copies of the same resolution and they agree to equally share the risk. With orthogonal fingerprint modulation, if the detection noise is i.i.d. Gaussian with zero mean and variance σ_n^2, then a guilty colluder $u^{(i)}$'s probability of being detected is

$$P_d^{sr} = Q\left(\frac{h - \sqrt{N_c}\sigma_w/K}{\sigma_n}\right) \tag{5}$$

and the probability to accuse an innocent user is $P_{fa}^{(i)} = Q(h/\sigma_n)$. Here, $Q(x) = (1/\sqrt{2\pi})\int_x^\infty e^{(-t^2/2)}dt$ is the Gauss tail function, h is a predetermined threshold, and N_c is the length of the fingerprint extracted from the colluded copy. We have $N_c = N_b$ if the colluded copy includes the base layer only ($f_c = f_b$), and $N_c = N_b + N_e$ when the colluded copy is of high resolution with both layers ($f_c = 1$). Here, the superscript "sr" denotes that all fingerprinted copies have the same resolution.[1]

With scalable video coding, colluders may receive fingerprinted copies of different resolutions. We consider the scenario where colluders in the same subgroup (with fingerprinted copies of the same resolution) agree to share the same risk. From the analysis in [20], with orthogonal fingerprint modulation, if the detection noise is i.i.d. Gaussian $\mathcal{N}(0, \sigma_n^2)$, for colluder $u^{(i)}$ who receives a low-resolution fingerprinted copy, his/her chance of being captured is

$$P_{d,c}^{b} = Q\left(\frac{h - \beta\sqrt{N_b}\sigma_w/K}{\sigma_n}\right). \tag{6}$$

Here, the superscript "b" indicates that colluder i is in the subgroup SC^b. If $u^{(i)}$ is innocent, his/her chance of being falsely accused is $P_{fa}^{(i)} = Q(h/\sigma_n)$.

For user $u^{(i)}$ who receives both layers from the content owner, note that the self-probing detector proposed in [22] has approximately the same performance as the optimum fingerprint detector with perfect information about the statistical means of the detection statistics. Therefore, during collusion, attackers should consider the worst case scenario and assume that the fingerprint detector can always select the optimum detection statistic with the largest mean. Therefore, if $u^{(i)}$ receives a high-resolution copy and participates in collusion, from (2) and (3), his/her chance of being detected is

$$P_{d,c}^{be} = \begin{cases} Q\left(\frac{h}{\sigma_n} - \frac{(1-\beta)N_b + N_e}{K^{be}\sqrt{N_b+N_e}} \cdot \frac{\sigma_w}{\sigma_n}\right), & \text{if } \beta \le \beta^+ \\ Q\left(\frac{h}{\sigma_n} - \frac{\sqrt{N_e}}{K^{be}} \cdot \frac{\sigma_w}{\sigma_n}\right), & \text{if } \beta > \beta^+. \end{cases} \tag{7}$$

Here, the superscript "be" means that colluder $i \in SC^{be}$. If $u^{(i)}$ is innocent, then the probability of falsely accusing him/her is $P_{fa}^{(i)} = Q(h/\sigma_n)$.

B. Loss $L^{(i)}$ and the Reward $R^{(i)}$

In this paper, we consider the scenario where $\{L^{(i)}\}$ are the same for all colluders. Furthermore, without loss of generality, we normalize $L^{(i)}$ to one for all $i \in SC$, which does not affect our analysis.

Depending on the video content itself, the reward can take different forms. For instance, for a commercial movie, the reward can be the money paid by the buyers who purchase the colluded copy. When defining the reward $R^{(i)}$, we consider the scenario where attackers receive more reward from collusion if the colluded copy has higher resolution and better quality. For instance, the pirated video with DVD quality would have higher value than that with VCD quality. With temporal scalable video coding, we use the frame rate to quantify the video quality, and let $R^{(i)}$ in (4) be an increasing function of the normalized temporal resolution of the colluded copy f_c. We consider a simplified case where colluders who receive the same quality copies will share the reward evenly. Hence, if all K colluders contribute fingerprinted copies of the same resolution, then they distribute the reward equally among themselves, and $R^{(i)} = f_c\theta/K$. Here, θ is a nonnegative real number that addresses the tradeoff between the risk that a colluder takes and the reward that he or she receives, and it has a smaller value when colluders emphasize more on risk minimization. Note that $\theta = 0$ corresponds to the scenario where colluders' only goal is to minimize their risk (the probability of being detected), which has been well studied in the literature. In this work, we consider the high-risk high-return scenario with a large θ. e.g., $\theta > 1$. In such a scenario, some attackers are willing to take the risk to gain potentially higher payoffs, and they should consider both

[1] With coded fingerprints, colluders' probability of being detected $P_d^{(i)}$ will be different. However, their utility function has the same form as in (4) and the same analysis can be used to study colluders' behavior in coded fingerprinting. For example, in Tardos code [25], $P_d^{(i)} \approx (1/K)$ when $K \le C$, where C is the designed maximal coalition size for a given code length N and a given false alarm probability P_{fa}. When $K > C$ and the code length N is large enough, each colluder's detection statistic approximately follows Gaussian distribution with mean and variance reciprocal to K. Hence $P_d^{(i)}$ can be approximated by a Gauss tail function [26], and the techniques proposed in later sections can also be used to study colluders' behavior there.

the risk and the reward when deciding whether to participate in collusion.

In this paper, we consider the scenario where colluders distribute the reward based on the resolution of each contributing copy, and where an attacker receives more reward if he/she contributes a copy of higher resolution. Following the general reward definition model proposed in [21], in this paper, we let

$$R^{(i)} = \frac{\left(f^{(i)}\right)^{\gamma}}{K^b(f_b)^{\gamma} + K^{be}}\theta. \tag{8}$$

Here, $\gamma \geq 0$ is a parameter that colluders use to adjust how they distribute the reward based on the resolution of each contributing copy. For colluder $i \in SC^{be}$ who contributes a high resolution copy, $R^{(i)}$ is an increasing function of γ and $u^{(i)}$ receives more reward when γ takes a larger value. Other definitions of the reward function can also be used, and the same procedure can be used to analyze colluder dynamics.

C. The Utility Function

To summarize, when all K colluders receive fingerprinted copies of the same resolution, colluder $u^{(i)}$'s utility function is

$$\nu^{sr} = -P_d^{sr} + \left(1 - P_d^{sr}\right)\frac{f_c\theta}{K} \tag{9}$$

where P_d^{sr} is in (5). If colluders receive copies of different resolutions, colluder $u^{(i)}$'s utility function is

$$\nu^{g} = -P_{d,c}^{g} + \left(1 - P_{d,c}^{g}\right)\frac{(f^g)^{\gamma}}{K^b(f_b)^{\gamma} + K^{be}}\theta \tag{10}$$

where $P_{d,c}^{g}$ is in (6) if $i \in SC^b$ and $P_{d,c}^{g}$ is in (7) if $i \in SC^{be}$. Here, the superscript "g" is the colluder subgroup index, and it is either "b" if $i \in SC^b$ or "be" if $i \in SC^{be}$.

D. Feasible Collusion

Given the assumption that colluders who receive copies of the same resolution agree to have the same risk and receive the same reward, to understand when and how the attackers collaborate with each other to form a coalition, we model the complex dynamics among colluders as a two-player game: colluders in SC^b act as a single player and they have the same utility ν^b, while those in SC^{be} act as a single player with payoff ν^{be}. From (10), the collusion parameter β determines colluders' probabilities of being detected and thus their utilities. During collusion, each attacker prefers the β that maximizes his/her own payoff, and the two subgroups of colluders negotiate with each other on the selection of β to resolve the conflict.

Given the utility function and the number of colluders in each subgroup, attackers first find the feasible set $\mathbb{S} = \{(\nu^b, \nu^{be}) \in \mathbb{R}^2 t\}$, where for every $(\nu^b, \nu^{be}) \in \mathbb{S}$, there exists at least one type of collusion that colluders in SC^b and SC^{be} can act together to select an appropriate collusion parameter β, and obtain the utilities ν^b and ν^{be}, respectively.

Among all possible solutions in the feasible set, attackers are especially interested in those in the Pareto optimal set $\mathbb{S}^+ \subseteq \mathbb{S}$. A solution is Pareto optimal if no one can further increase his or her utility without decreasing others'. In a bargaining situation like this, colluders would always like to settle at a Pareto optimal point. From (7) and (10), in the colluder game, the Pareto optimal set corresponds to the solutions where attackers select $0 \leq \beta \leq \beta^+ = \sqrt{N_b + N_e}(\sqrt{N_b + N_e} - \sqrt{N_e})/N_b$, that is, $\mathbb{S}^+ = \{(\nu^b, \nu^{be}) \in \mathbb{S} : 0 \leq \beta \leq \beta^+\}$. This is because, for colluder $u^{(i)} \in SC^{be}$, when $\beta \geq \beta^+$, $u^{(i)}$'s probability of being detected $P_d^{(i)}$ in (7) is a constant of β. Therefore, from (10), ν^{be} is the same for all $\beta \geq \beta^+$. Meanwhile, for colluder $j \in SC^b$, $P_d^{(j)}$ in (6) is an increasing function of β, and thus, ν^b is a decreasing function of β. So colluders in SC^b are not willing to contribute more than β^+ to the base layer of the colluded copy, and for $\beta \in [\beta^+, 1]$, colluders in SC^b prefer β^+ to improve their utility ν^b without decreasing ν^{be}, the utility of those colluders in SC^{be}. When $0 \leq \beta \leq \beta^+$, ν^{be} is an increasing function of β while ν^b is a decreasing function of β, and $0 \leq \beta \leq \beta^+$ is the necessary and sufficient condition for Pareto optimality [21].

In addition, note that attackers will collude with each other if and only if collusion helps increase their utilities, and they are interested in solutions in $\mathbb{S}^+$ that give them higher payoffs when compared with the scenario where they do not cooperate with each other.

- First, if attacker $u^{(i)}$ does not participate in collusion and does not use multimedia content illegally, his/her payoff is zero. Thus, $u^{(i)}$ colludes with other attackers only if he/she receives positive payoff from collusion, and colluders are only interested in solutions in $\mathbb{S}^+$ where $\nu^b \geq 0$ and $\nu^{be} \geq 0$.
- Furthermore, note that one possible outcome of the bargaining between SC^b and SC^{be} is that they do not reach an agreement. In such a scenario, attackers will only collude with their fellow attackers in the same subgroup, and SC^b and SC^{be} do not cooperate with each other. Let ν_{nc}^b denote the utility of a colluder in SC^b if he/she colludes with attackers in SC^b only but not those in SC^{be}; and similarly, ν_{nc}^{be} is the utility of an attacker in SC^{be} if he/she colludes with attackers in SC^{be} only but not SC^b. Here, the subscript 'nc' means no cooperation. Therefore, SC^b and SC^{be} will collude with each other only if the two-stage collusion in Section II-A.2 increases both players' payoffs, and they look for solutions in $\mathbb{S}^+$ where $\nu^b \geq \nu_{nc}^b$ and $\nu^{be} \geq \nu_{nc}^{be}$.

The above analysis helps colluders further narrow down the feasible set to

$$\begin{aligned}\mathbb{S}_p = \Big\{(\nu^b, \nu^{be}) \in \mathbb{S} : 0 \leq &\beta \leq \beta^+ \\ &\nu^b \geq \underline{\nu}^b \triangleq \max\left(\nu_{nc}^b, 0\right) \\ &\nu^{be} \geq \underline{\nu}^{be} \triangleq \max\left(\nu_{nc}^{be}, 0\right)\Big\}.\end{aligned} \tag{11}$$

With the constraint $0 \leq \beta \leq \beta^+$, every collusion point in the feasible set $\mathbb{S}_p$ will be Pareto optimal, where reasonable colluders will all go.

IV. Colluder Dynamics in Multiuser Collusion

In this section, we analyze *when* attackers will collude with others who have copies of the same quality, and investigate the optimum number of colluders that maximizes each colluder's payoff.

A. Colluders' Payoff Functions

As an example and without loss of generality, we assume that all attackers receive high resolution copies with both layers,

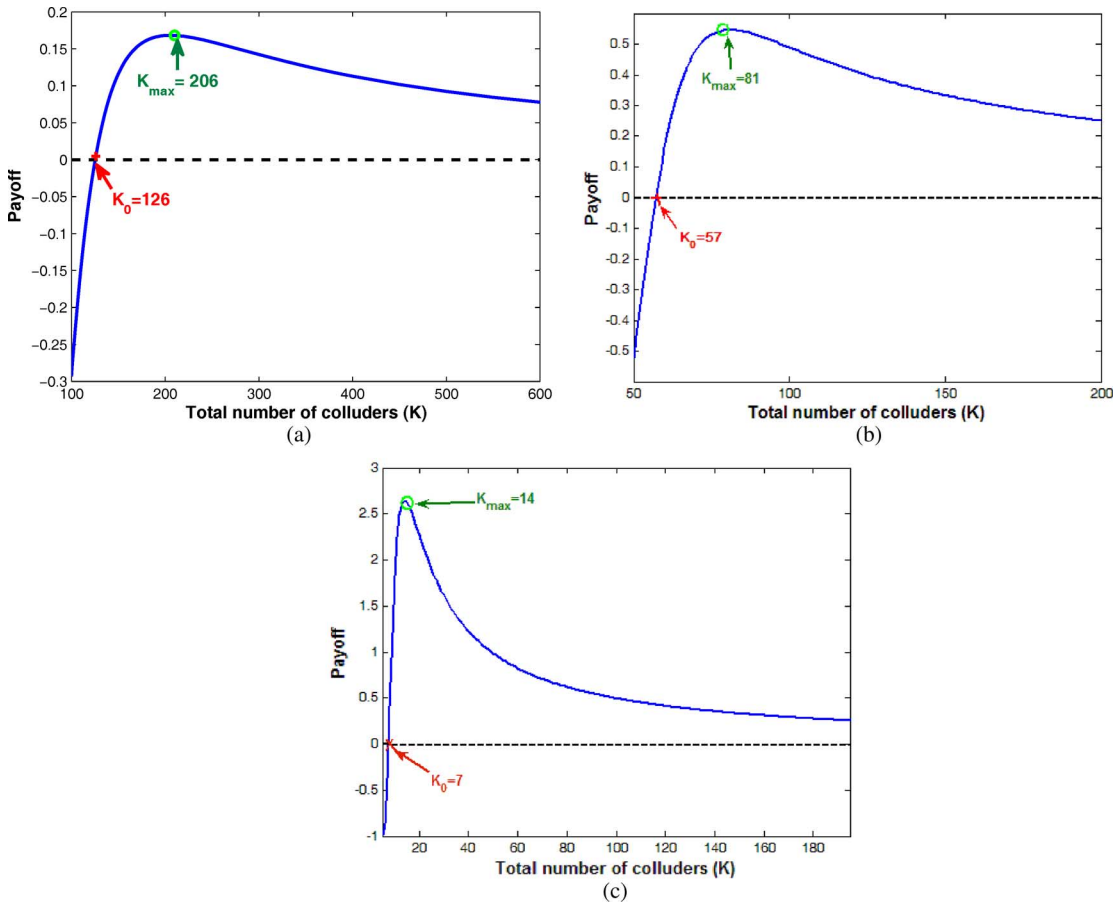


Fig. 1. $\nu^{(i)}$ when all colluders receive fingerprinted copies of high resolution. $N_b = N_e = 50\,000$ and $\theta = 50$. (a) $P_{fa} = 10^{-3}$, $\sigma_n^2 = \sigma_w^2$. (b) $P_{fa} = 10^{-8}$, $\sigma_n^2 = \sigma_w^2$. (c) $P_{fa} = 10^{-8}$, $\sigma_n^2 = 10\sigma_w^2$.

and they generate a colluded copy of high resolution, that is, $K = K^{be}$ and $f_c = 1$. The analysis is similar for the scenario where all fingerprinted copies have the base layer only and thus omitted. In such a scenario, since all copies have the same resolution, there is no bargaining in collusion, and attackers simply average all copies that they have with equal weights.

Fig. 1 shows an example of $\nu^{(i)}$ versus the total number of colluders K. In Fig. 1, the lengths of the fingerprints embedded in the base layer and the enhancement layer are $N_b = 50\,000$ and $N_e = 50\,000$, respectively. In Fig. 1, we use $\theta = 50$ as an example to illustrate colluders' payoffs, and we observe similar trends for other values of θ. The threshold h is selected so that the probability of falsely accusing an innocent user $P_{fa} = Q(h/\sigma_n)$ is 10^{-3} in Fig. 1(a) and, $P_{fa} = 10^{-8}$ in Fig. 1(b) and (c). We let $\sigma_w^2 = \sigma_n^2$ in Fig. 1(a) and (b), and $\sigma_n^2 = 10\sigma_w^2$ in Fig. 1(c). We can see from Fig. 1 that the payoff versus total number of colluders follows the same trend with different P_{fa} and different values of σ_w^2/σ_n^2. From Fig. 1(a), when $K < 126$, $\nu^{(i)} < 0$ due to $u^{(i)}$'s large probability of being detected. In this scenario, colluders may not want to use multimedia illegally since it is too risky. Furthermore, from Fig. 1(a), colluding with more attackers does not always increase $u^{(i)}$'s payoff, and $\nu^{(i)}$ becomes a decreasing function of K when there are more than 206 attackers.

Let $K_0 \triangleq \{K : \nu^{(i)}(K-1) < 0, \nu^{(i)}(K) \geq 0\}$ be the smallest K that gives $u^{(i)}$ a non-negative payoff. Attackers will collude with each other if and only if there are more than K_0 colluders and when they receive positive payoffs from collusion. Also, we define $K_{\max} \triangleq \arg_{K \geq K_0} \max \nu^{(i)}$ as the optimum K that maximizes colluder $u^{(i)}$'s utility when all attackers receive copies of the same resolution. A colluder should find a total of $K_{\max}$ attackers if possible to maximize his/her payoff. In the example with $P_{fa} = 10^{-3}$ and $\sigma_n^2 = \sigma_w^2$ in Fig. 1(a), $K_0 = 126$ and $K_{\max} = 206$.

B. Analysis of K_0 and $K_{\max}$

Given N_b, N_e and θ, to find K_0, we first extend the support of K from integers to real numbers, and then solve the equation $\nu^{(i)}(\tilde{K}_0) = 0$. Note that K_0 is defined as the smallest integer that makes the payoff $\nu^{(i)}$ non-negative. Therefore, $K_0 = \lceil \tilde{K}_0 \rceil$. To find $K_{\max}$, we first find the real number $\tilde{K}_{\max}$ that satisfies $(\partial \nu^{(i)}/\partial K)|_{K=\tilde{K}_{\max}} = 0$. By smoothness, we have $K_{\max} = \arg\max_{\{\lfloor \tilde{K}_{\max} \rfloor, \lceil \tilde{K}_{\max} \rceil\}} \nu^{(i)}$.

Fig. 2 shows K_0 for different values of θ and f_c. The system setup in Fig. 2 is similar to that in Fig. 1. Fig. 2 suggests that K_0 is a decreasing function of θ. As an example, when $f_c = 1$ and $P_{fa} = 10^{-3}$, K_0 drops from 235 to 103 when θ increases from 10 to 100. In addition, from Fig. 2, K_0 takes a smaller value if colluders generate a colluded copy of lower resolution. For example, with $\theta = 50$ and $P_{fa} = 10^{-3}$, $K_0 = 126$ when $f_c = 1$ and $K_0 = 100$ when $f_c = 0.5$.

Fig. 3 shows $K_{\max}$ as a function of θ when the colluded copy has high and low resolutions, respectively. The system setup is

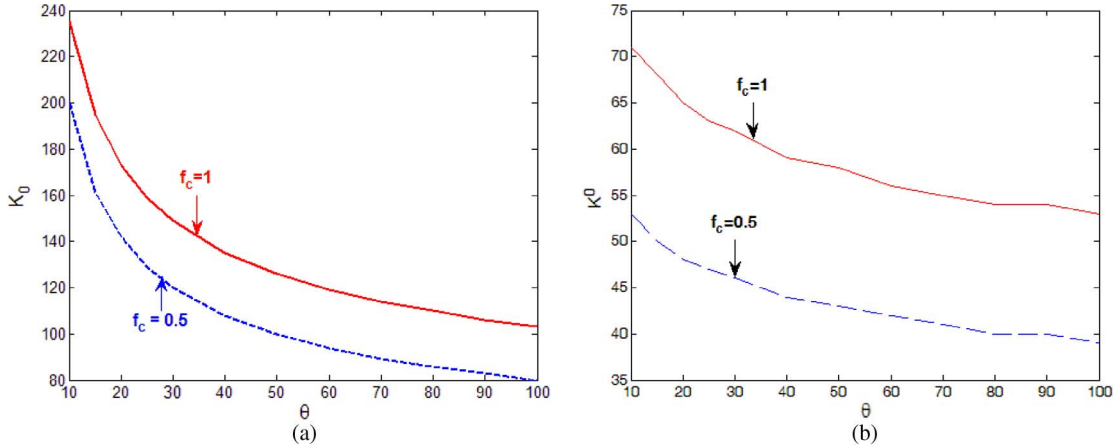


Fig. 2. K_0 versus θ. $N_b = N_e = 50\,000$, $\sigma_w^2 = \sigma_n^2$. (a) $P_{fa} = 10^{-3}$. (b) $P_{fa} = 10^{-8}$.

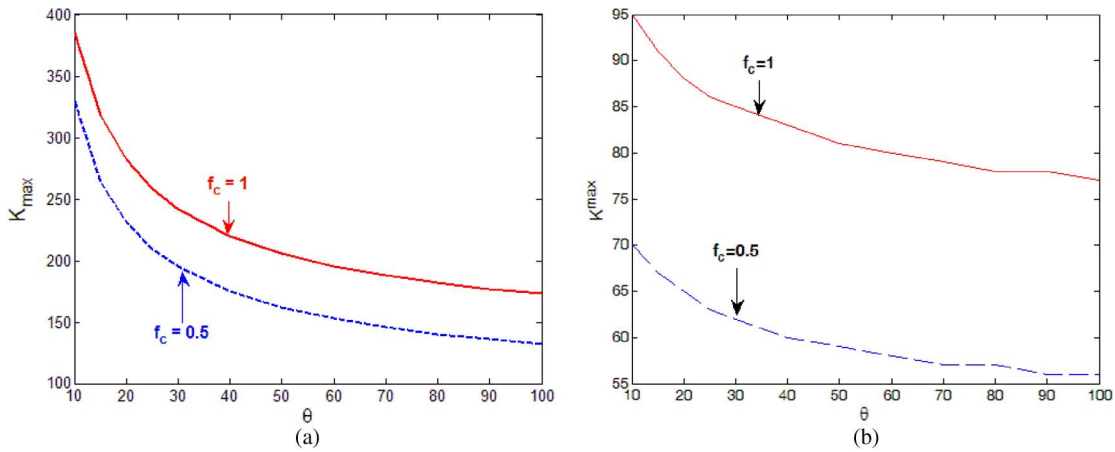


Fig. 3. $K_{\max}$ versus θ. $N_b = N_e = 50\,000$, $\sigma_w^2 = \sigma_n^2$. (a) $P_{fa} = 10^{-3}$. (b) $P_{fa} = 10^{-8}$.

the same as in Fig. 2. From Fig. 3, $K_{\max}$ takes a smaller value when the colluded copy has a lower resolution. For example, in Fig. 3(a), with $\theta = 50$ and $P_{fa} = 10^{-3}$, $K_{\max} = 206$ when the colluded copy has high resolution, and $K_{\max} = 162$ when $f_c = 0.5$. Furthermore, $K_{\max}$ is a decreasing function of θ. For example, with $f_c = 1$ and $P_{fa} = 10^{-3}$, $K_{\max} = 385$ when $\theta = 10$ and $K_{\max} = 173$ when $\theta = 100$. This is because, when θ takes a smaller value and when attackers emphasize more on risk minimization, they prefer to collude with more people to lower their risk.

To summarize, when all attackers receive copies of the same resolution, they collude with each other if and only if the total number of colluders is larger than K_0 and when all attackers receive positive payoffs. In addition, an attacker should try to find a total of $K_{\max}$ colluders if possible to maximize his/her payoff.

V. Colluder Dynamics in Multi-Resolution Multiuser Collusion

In this section, we consider the scenario where colluders receive fingerprinted copies of different resolutions, analyze when attackers will collude with other attackers with different quality copies, and investigate how an attacker selects his/her fellow attackers to maximize his/her payoff.

A. Analysis of Feasible Collusion

In Section III-D, multiuser collusion is modeled as a two-player game, in which the two subgroups of colluders, SC^b and SC^{be}, negotiate with each other to reach an agreement on fair distribution of the risk and the reward. To understand the dynamics among colluders, the first step is to analyze the Pareto-optimal feasible set $\mathbb{S}_p$ in (11) and to investigate under what conditions attackers will collude with each other.

1) Colluders' Payoff Functions: From Section III-D, one possible outcome of the bargaining between SC^b and SC^{be} is that they do not reach an agreement. In such a scenario, attackers only collude with their fellow attackers in the same subgroup, and SC^b and SC^{be} do not cooperate with each other. Given N_b, N_e, K^b and K^{be}, if an attacker in SC^b colludes with those in SC^b only, following the same analysis as in Section IV, his or her utility is

$$\begin{aligned} \nu_{nc}^b &= -P_{d,nc}^b + \left(1 - P_{d,nc}^b\right) R_{nc}^b \\ P_{d,nc}^b &= Q\left(\frac{h}{\sigma_n} - \frac{\sqrt{N_b}\sigma_w}{K^b \sigma_n}\right) \\ &= Q(a - b_b/K^b) \\ R_{nc}^b &= \frac{\theta f_b}{K^b}. \end{aligned} \tag{12}$$

In (12), $a = h/\sigma_n$ and $b_b = \sqrt{N_b}\sigma_w/\sigma_n$. Similarly, if an attacker in SC^{be} colludes with those in SC^{be} only, his or her payoff is

$$\begin{aligned}\nu_{nc}^{be} &= -P_{d,nc}^{be} + \left(1 - P_{d,nc}^{be}\right) R_{nc}^{be} \\ P_{d,nc}^{be} &= Q\left(\frac{h}{\sigma_n} - \frac{\sqrt{N_b + N_e}\sigma_w}{K^{be}\sigma_n}\right) \\ &= Q\left(a - b_s/K^{be}\right) \\ R_{nc}^{be} &= \frac{\theta}{K^{be}}. \end{aligned} \tag{13}$$

In (13), $b_s = \sqrt{N_b + N_e}\sigma_w/\sigma_n$.

If SC^b and SC^{be} collaborate with each other and select the collusion parameter β, following the analysis in Section III, for an attacker $i \in SC^b$, his or her utility is

$$\begin{aligned}\nu^{b} &= -P_{d,c}^{b} + \left(1 - P_{d,c}^{b}\right) R_{c}^{b} \\ P_{d,c}^{b} &= Q\left(\frac{h}{\sigma_n} - \frac{\beta\sqrt{N_b}}{K^b} \cdot \frac{\sigma_w}{\sigma_n}\right) \\ &= Q\left(a - \beta\frac{b_b}{K^b}\right) \\ R_{c}^{b} &= \frac{(f_b)^\gamma \theta}{K^b (f_b)^\gamma + K^{be}}. \end{aligned} \tag{14}$$

Similarly, for $0 \le \beta \le \beta^+$, an attacker $i \in SC^{be}$'s payoff is

$$\begin{aligned}\nu^{be} &= -P_{d,c}^{be} + \left(1 - P_{d,c}^{be}\right) R_{c}^{be} \\ P_{d,c}^{be} &= Q\left(\frac{h}{\sigma_n} - \frac{(1-\beta)N_b + N_e}{K^{be}\sqrt{N_b + N_e}} \cdot \frac{\sigma_w}{\sigma_n}\right) \\ &= Q\left(a - \frac{b_s}{K^{be}} + \beta\frac{b_{be}}{K^{be}}\right) \\ R_{c}^{be} &= \frac{\theta}{K^b (f_b)^\gamma + K^{be}}. \end{aligned} \tag{15}$$

In (15), $b_{be} = N_b\sigma_w/\sqrt{N_b + N_e}\sigma_n$.

From Section III-D, among all the possible solutions $\{(\nu^b, \nu^{be})\}$ in the feasible set $\mathbb{S}$, colluders are only interested in those in $\mathbb{S}_p = \{(\nu^b, \nu^{be}) \in \mathbb{S} : \nu^b \ge \underline{\nu}^b = \max(0, \nu_{nc}^b), \nu^{be} \ge \underline{\nu}^{be} = \max(0, \nu_{nc}^b), 0 \le \beta \le \beta^+\}$, where cooperation helps both SC^b and SC^{be} increase their payoffs.

- From (14), $P_{d,c}^b$ is an increasing function of β and, ν^b is a decreasing function of β. Let $\bar{\beta}$ be the β that makes ν^b equal to $\underline{\nu}^b$, that is, $\nu^b(\bar{\beta}) = \underline{\nu}^b$. Then, the constraint $\nu^b \ge \underline{\nu}^b$ is equivalent to $\beta \le \bar{\beta}$.
- Similarly, from (15), $P_{d,c}^{be}$ is a decreasing function of β, and thus ν^{be} is an increasing function of β. Let $\underline{\beta}$ be the β that makes ν^{be} equal to $\underline{\nu}^{be}$, that is, $\nu^{be}(\underline{\beta}) = \underline{\nu}^{be}$. Therefore, the constraint $\nu^{be} \ge \underline{\nu}^{be}$ is equivalent to $\beta \ge \underline{\beta}$.
- Furthermore, note that $\underline{\beta}$ is the minimum β that colluders in SC^b need to contribute for colluders in SC^{be} to consider cooperation. Selecting $\beta = 0$ corresponds to the scenario where SC^b contributes nothing but still share some reward, which is unacceptable to SC^{be}. Therefore, $\underline{\beta} > 0$.

From the above analysis, we can rewrite $\mathbb{S}_p$ as $\mathbb{S}_p = \{(\nu^b, \nu^{be}) \in \mathbb{S} : \underline{\beta} \le \beta \le \min(\bar{\beta}, \beta^+)\}$. When attackers receive fingerprinted copies of different resolutions, the two subgroups of colluders SC^b and SC^{be} will collude with each other if and only if there exists at least one β such that $\underline{\beta} \le \beta \le \min(\bar{\beta}, \beta^+)$, or equivalently, when $\mathbb{S}_p$ is not empty.

2) Lower and Upper Bounds of the Collusion Parameter: To further understand under what conditions SC^b and SC^{be} will cooperate with each other, we will first analyze $\underline{\beta}$ and $\bar{\beta}$.

From the previous discussion, given N_b, N_e, K^b and K^{be}, colluders should select β such that

$$\nu^b(\beta) = -P_{d,c}^b(\beta) + \left[1 - P_{d,c}^b(\beta)\right] R_c^b \ge \underline{\nu}^b = \max\left(0, \nu_{nc}^b\right) \tag{16}$$

where $P_{d,c}^b(\beta)$ and R_c^b are in (14). Consequently, we have

$$P_{d,c}^b(\beta) = Q\left(a - \frac{\beta b_b}{K^b}\right) \le \frac{R_c^b - \underline{\nu}^b}{R_c^b + 1}$$

or equivalently

$$\beta \le \bar{\beta} = \left[a - Q^{-1}\left(\frac{R_c^b - \underline{\nu}^b}{R_c^b + 1}\right)\right] \frac{K^b}{b_b}. \tag{17}$$

Similarly, given N_b, N_e, K^b, and K^{be}, colluders should select β such that

$$\nu^{be}(\beta) = -P_{d,c}^{be}(\beta) + \left[1 - P_{d,c}^{be}(\beta)\right] R_c^{be} \ge \underline{\nu}^{be} = \max\left(0, \nu_{nc}^{be}\right) \tag{18}$$

where $P_{d,c}^{be}(\beta)$ and R_c^{be} are in (15). Therefore, we have

$$P_{d,c}^{be}(\beta) = Q\left(a - \frac{\sqrt{N_b + N_e}\sigma_w}{K^{be}\sigma_n} + \frac{\beta b_{be}}{K^{be}}\right) \le \frac{R_c^{be} - \underline{\nu}^{be}}{R_c^{be} + 1}$$

or equivalently

$$\beta \ge \underline{\beta} = \frac{N_b + N_e}{N_b} + \left[Q^{-1}\left(\frac{R_c^{be} - \underline{\nu}^{be}}{R_c^{be} + 1}\right) - a\right] \frac{K^{be}}{b_{be}}. \tag{19}$$

Fig. 4 shows examples of $\underline{\beta}$ and $\bar{\beta}$. The system setup is similar to that in Fig. 1(a). $K^{be} = 120$ in Fig. 1(a), and $K^b = 50$ in Fig. 4(b). From Fig. 4(a), $\bar{\beta} < \underline{\beta}$ when $K^b < 9$, and $\underline{\beta} > \beta^+$ when $K^b > 358$. Therefore, in this example where K^{be} is fixed as 120, $\mathbb{S}_p \ne \emptyset$ if and only if $9 \le K^b \le 358$. Similarly, from Fig. 4(b), $\underline{\beta} > \bar{\beta}$ if $K^{be} < 94$ or $K^{be} > 207$. Thus, when $K^b = 50$ is fixed, SC^{be} and SC^b will collude with each other if and only if $94 \le K^{be} \le 207$. Note that in Fig. 4(b), $\underline{\beta}$ changes its characteristics around the point $K^{be} = 126$. This is because $K_0(f_c = 1) = 126$ from Fig. 1(a) and, therefore, $\underline{\nu}^{be} = 0$ when $K^{be} < 126$ and $\underline{\nu}^{be} > 0$ when $K^{be} \ge 126$, which affects $\underline{\beta}$ in (19).

3) Analysis of the Number of Colluders: From Fig. 4, given N_b, N_e and θ, for some pairs of (K^b, K^{be}), $\mathbb{S}_p$ may be empty and thus, SC^b and SC^{be} will not cooperate. Define $\mathbb{K}_p \triangleq \{(K^b, K^{be}) : \mathbb{S}_p \ne \emptyset\}$ as the set including all pairs of (K^b, K^{be}) where $\mathbb{S}_p$ is not empty and where SC^b and SC^{be} will collude with each other.

Given N_b, N_e and θ, SC^b and SC^{be} will collude with each other if and only if $\mathbb{S}_p \ne \emptyset$, that is, when $\underline{\beta} \le \beta^+$ and $\underline{\beta} \le \bar{\beta}$.

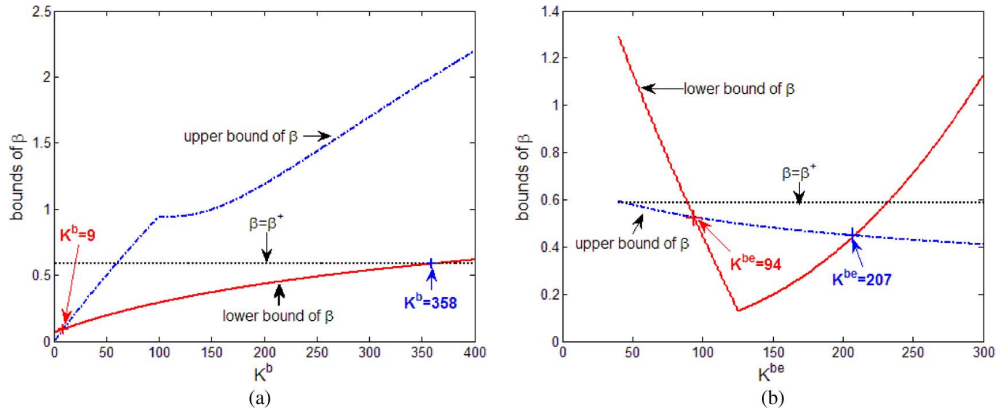


Fig. 4. $\bar{\beta}$ in (17) and $\underline{\beta}$ in (19). $N_b = N_e = 50\,000$, $\sigma_w^2 = \sigma_n^2 = 1$, $P_{fa} = 10^{-3}$, $\theta = 50$, and $\gamma = 1/3$. (a): $K^{be} = 120$. (b): $K^b = 50$.

Since ν^{be} in (15) is an increasing function of β, to ensure $\underline{\beta} \leq \beta^+$, it is required that

$$\nu^{be}(\beta^+) = -P_{d,c}^{be}(\beta^+) + \left[1 - P_{d,c}^{be}(\beta^+)\right] R_c^{be} \geq \nu^{be}(\underline{\beta}) = \underline{\nu}^{be}$$

or equivalently

$$K^b \leq K^{b'}(K^{be}) \triangleq \frac{\theta\left(1 - P_{d,c}^{be}(\beta^+)\right)}{\left(\underline{\nu}^{be} + P_{d,c}^{be}(\beta^+)\right)(f_b)^\gamma} - \frac{K^{be}}{(f_b)^\gamma}. \quad (20)$$

From (17) and (19), to ensure $\underline{\beta} \leq \bar{\beta}$, (K^b, K^{be}) must satisfy

$$\underline{\beta} = \frac{N_b + N_e}{N_b} + \left[Q^{-1}\left(\frac{R_c^{be} - \underline{\nu}^{be}}{R_c^{be} + 1}\right) - a\right]\frac{K^{be}}{b_{be}} \leq \bar{\beta} = \left[a - Q^{-1}\left(\frac{R_c^b - \underline{\nu}^b}{R_c^b + 1}\right)\right]\frac{K^b}{b_b}. \quad (21)$$

Combining (20) and (21), we have

$$\mathbb{K}_p = \Bigg\{(K^b, K^{be}) : K^b \geq 1, K^{be} \geq 1, K^b \leq \frac{\theta\left(1 - P_{d,c}^{be}(\beta^+)\right)}{\left(\underline{\nu}^{be} + P_{d,c}^{be}(\beta^+)\right)(f_b)^\gamma} - \frac{K^{be}}{(f_b)^\gamma}, \frac{N_b + N_e}{N_b} + \left[Q^{-1}\left(\frac{R_c^{be} - \underline{\nu}^{be}}{R_c^{be} + 1}\right) - a\right]\frac{K^{be}}{b_{be}} \leq \left[a - Q^{-1}\left(\frac{R_c^b - \underline{\nu}^b}{R_c^b + 1}\right)\right]\frac{K^b}{b_b}\Bigg\}. \quad (22)$$

The shaded area in Fig. 5(a) shows an example of $\mathbb{K}_p$. At point "A" in Fig. 5(a), when $K^{be} < 91$, no matter which value K^b takes, $\mathbb{S}_p$ is always empty and attackers will not collude with each other. Similarly, when $K^{be} > 226$ [point "B" in Fig. 5(a)], no matter how many attackers are in SC^b and how they select β, cooperation between SC^b and SC^{be} cannot improve all colluders' payoffs. Furthermore, when $K^b > 431$ [point "C" in Fig. 5(a)]. SC^b and SC^{be} will not collude with each other. In addition, when $125 \leq K^{be} \leq 226$, $(K^b = 1, K^{be})$ is in the feasible region $\mathbb{K}_p$ and the lower bound of K^b is 1. To quantify the above boundary points of $\mathbb{K}_p$, we define

$$\begin{aligned}\underline{K}^{be} &\triangleq \min\left\{K^{be} : \exists K^b \text{s.t.}(K^b, K^{be}) \in \mathbb{K}_p\right\}\\ \bar{K}^{be} &\triangleq \max\left\{K^{be} : \exists K^b \text{s.t.}(K^b, K^{be}) \in \mathbb{K}_p\right\}\\ \bar{K}^b &\triangleq \max\left\{K^b : \exists K^{be} \text{s.t.}(K^b, K^{be}) \in \mathbb{K}_p\right\}. \end{aligned} \quad (23)$$

In the example in Fig. 5(a), $\underline{K}^{be} = 91$, $\bar{K}^{be} = 226$, and $\bar{K}^b = 431$. Fig. 5(b) and (c) show the feasible region $\mathbb{K}_p$ when $\theta = 150$ and $P_{fa} = 10^{-8}$, respectively, where we observe the same trend as in Fig. 5(a). From Fig. 5, when θ takes a smaller value and colluders emphasize more on risk minimization, they prefer to collude with more people to reduce their risk of being detected and more colluders join the coalition. This is similar to the single-resolution case. Note that it is possible that $\mathbb{K}_p$ is empty in some scenarios. For example, with the same system setup as in Fig. 5(c), $\max_{K^{be}}\{K^{b'}(K^{be})\} = 0.0088 < 1$ when $(\sigma_n^2/\sigma_w^2) = 100$ and, therefore, $\mathbb{K}_p = \emptyset$. In such a case, colluders in SC^{be} will never cooperate with those in SC^b, since for any $K^b \geq 1$, there is no β in the range $[0, \beta^+]$ that can increase their utility ν^{be}.

Note that for colluders, Fig. 5 and (23) show that if $K^b > \bar{K}^b$, $K^{be} < \underline{K}^{be}$, or $K^{be} > \bar{K}^{be}$, it is impossible to find a β that increases all colluders' payoffs, and SC^b and SC^{be} will not cooperate with each other. Therefore, during collusion, as a preliminary step, colluders should first check that $K^b \leq \bar{K}^b$ and $\underline{K}^{be} \leq K^{be} \leq \bar{K}^{be}$. Then, they should ensure that (K^b, K^{be}) is in the set $\mathbb{K}_p$ defined in (23), and guarantee that there exists at least one β that increases both SC^b and SC^{be}'s payoffs.

From traitor tracing perspective, Fig. 5 shows that in the scenarios considered in this work, we are more likely to see colluder groups with a few dozen to a few hundred colluders. This is because such group sizes ensure the feasibility and Pareto-optimality of collusion and improve all colluders' utilities, where all colluders will go for. Thus, a digital fingerprinting system designer should focus on such colluder group size and design collusion-resistant fingerprinting systems accordingly.

In the following section, we will analyze the boundary points of $\mathbb{K}_p$ ($\underline{K}^{be}$, $\bar{K}^{be}$, and $\bar{K}^b$) in details.

a) Lower Bound of K^{be}: Using exhaustive search, we find that at point "A" in Fig. 5(a), $K^b = 56$ and $K^{be} = 91$. To have a better understanding of $\underline{K}^{be}$, Fig. 6 plots $\underline{\beta}$ and $\bar{\beta}$ around

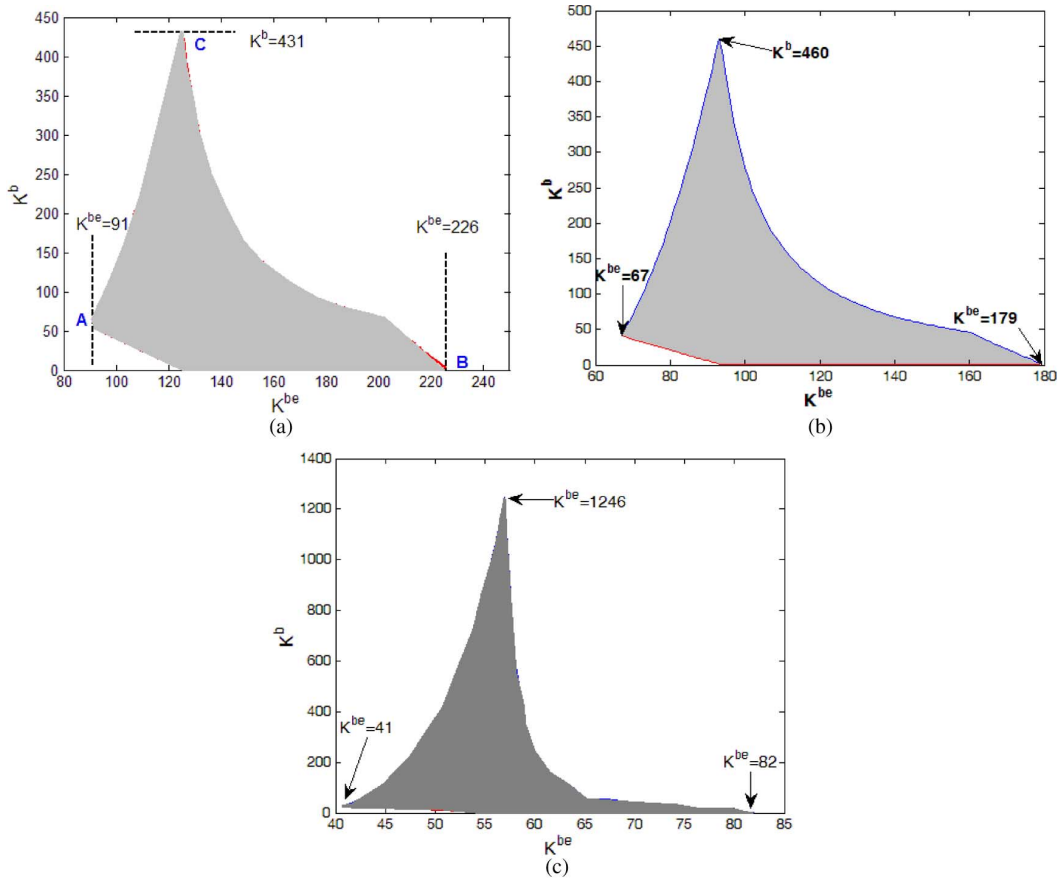


Fig. 5. An example of $\mathbb{K}_p$. $N_b = N_e = 50\,000$, $\sigma_n^2 = \sigma_w^2$, and $\gamma = 1/3$. (a) $\theta = 50$, $P_{fa} = 10^{-3}$. (b) $\theta = 150$, $P_{fa} = 10^{-3}$. (c) $\theta = 50$, $P_{fa} = 10^{-8}$.

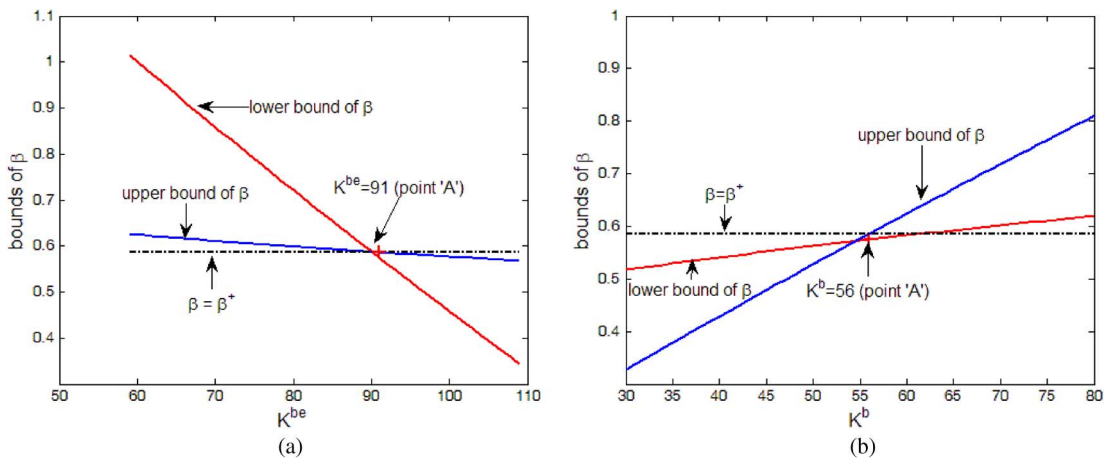


Fig. 6. $\underline{\beta}$ and $\bar{\beta}$ at point "A" in Fig. 5(a). $N_b = N_e = 50\,000$, $\sigma_w^2 = \sigma_n^2 = 1$, $\gamma = 1/3$, $P_{fa} = 10^{-3}$, and $\theta = 50$. (a) $K^b = 56$. (b) $K^{be} = 91$.

the point ($K^b = 56$,$K^{be} = 91$). Fig. 6 suggests that, at point "A", $\underline{\beta} = \bar{\beta} = \beta^+$, and $\mathbb{S}_p$ has only one item, which is $\mathbb{S}_p = \{(\nu^b, \nu^{be}) : \beta = \beta^+\}$. Therefore, to find $\underline{K}^{be}$, we first extend the support of (K^b, K^{be}) to the first quadrant in the 2-D plane, and solve the equation $\underline{\beta}(\tilde{K}^b, \tilde{K}^{be}) = \bar{\beta}(\tilde{K}^b, \tilde{K}^{be}) = \beta^+$. By smoothness, we have $\underline{K}^{be} = \lceil \tilde{K}^{be} \rceil$. Using Fig. 5(a) as an example, given the parameters $N_b = N_e = 50\,000$, $\gamma = 1/3$, $\theta = 50$ and $P_{fa} = 10^{-3}$, the solution to the equation $\underline{\beta} = \bar{\beta} = \beta^+$ is ($\tilde{K}^b = 55.88$, $\tilde{K}^{be} = 90.15$). Thus, $\underline{K}^{be} = \lceil \tilde{K}^{be} \rceil = 91$, and it is consistent with the result we find using exhaustive search. In the example in Fig. 5(c) where $P_{fa} = 10^{-8}$, the solution is ($\tilde{K}^b = 24.47$, $\tilde{K}^{be} = 40.68$) and $\underline{K}^{be} = \lceil \tilde{K}^{be} \rceil = 41$, which is consistent with the result $\underline{K}^{be} = 41$ that we find using exhaustive search.

b) Upper Bound of K^{be}: To analyze $\bar{K}^{be}$, using exhaustive search, we find that at point "B" in Fig. 5(a), $K^b = 1 < K_0(f_c = f_b) = 100$ and $K^{be} = 226 > K_0(f_c = 1) = 126$. Fig. 7 suggests that, at this point, $\underline{\beta} = \bar{\beta}$, and $\mathbb{S}_p = \{(\nu^b, \nu^{be}) : \underline{\beta} = \bar{\beta}\}$ has only one entry. Also, from Fig. 7(b), when $K^{be} = \bar{K}^{be}$, if SC^b has more than one attacker (that is, $K^b \geq 2$), there is no β that can improve both SC^{be} and SC^b's payoffs. Therefore, to find $\bar{K}^{be}$, we first extend the support of K^{be} from integers to real numbers and find point 'B' by solving $\underline{\beta}(K^b = 1, \tilde{K}^{be}) = \bar{\beta}(K^b = 1, \tilde{K}^{be})$. By smoothness,

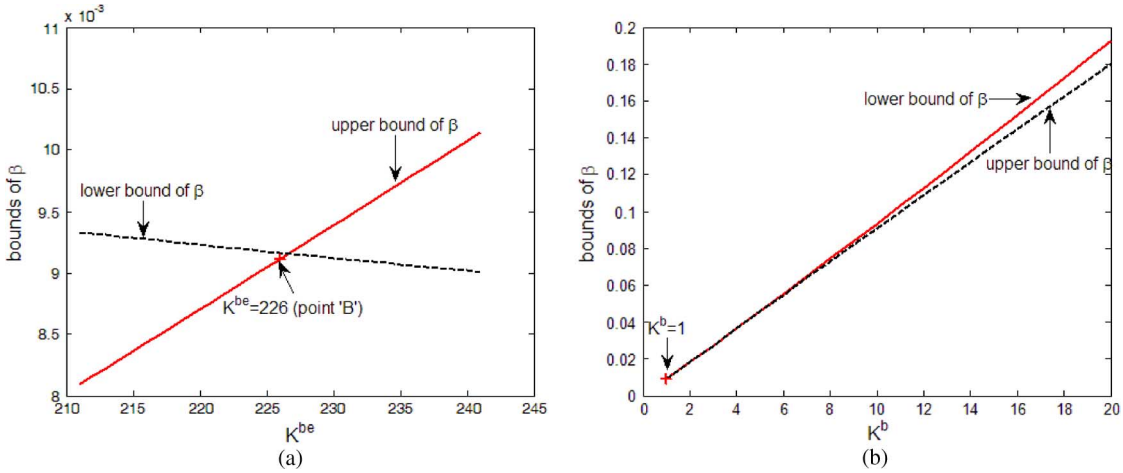


Fig. 7. $\underline{\beta}$ and $\bar{\beta}$ at point 'B' in Fig. 5(a). $N_b = N_e = 50\,000$, $\sigma_w^2 = \sigma_n^2 = 1$, $\gamma = 1/3$, $P_{fa} = 10^{-3}$, and $\theta = 50$. (a) $K^b = 1$, (b) $K^{be} = 226$.

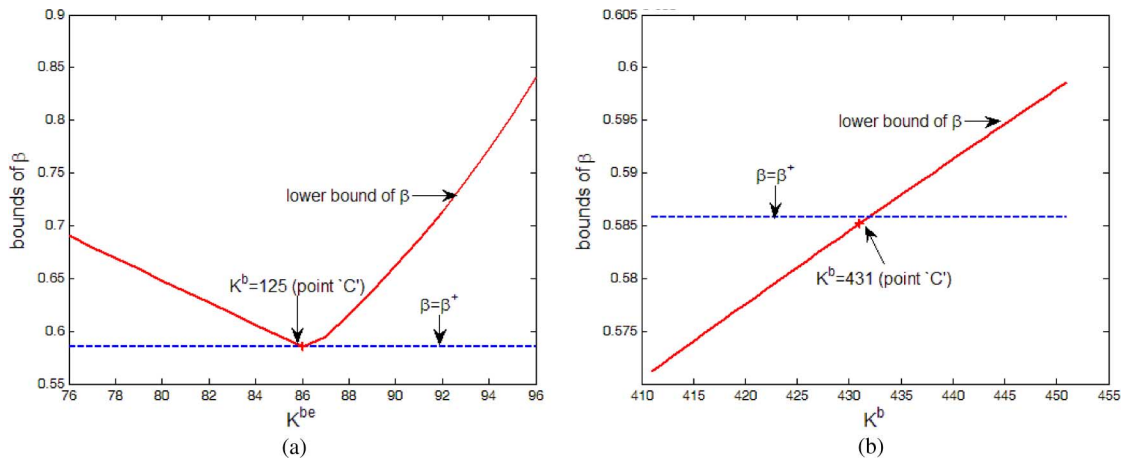


Fig. 8. $\underline{\beta}$ and $\bar{\beta}$ at point "C" in Fig. 5(a). $N_b = N_e = 50\,000$, $\sigma_w^2 = \sigma_n^2 = 1$, $\gamma = 1/3$, $P_{fa} = 10^{-3}$, and $\theta = 50$. (a) $K^b = 125$, (b) $K^{be} = 431$.

we have $\bar{K}^{be} = \lfloor \tilde{K}^{be} \rfloor$. As an example, given the system setup in Fig. 5(a), the numerical solution to $\underline{\beta} = \bar{\beta}$ with $K^b = 1$ is $\tilde{K}^{be} = 226.64$ and thus $\bar{K}^{be} = \lfloor 226.64 \rfloor = 226$. It is consistent with the result we found using exhaustive search. Similarly, for the example in Fig. 5(c) with $P_{fa} = 10^{-8}$, $\tilde{K}^{be} = 82.53$ and $\bar{K}^{be} = \lfloor 82.53 \rfloor = 82$, which is consistent with the exhaustive search result.

c) Upper Bound of K^b: $\bar{K}^b$: At point "C" in Fig. 5(a), we find $K^b = 431$ and $K^{be} = 125$ using exhaustive search and $\underline{\beta} = \beta^+$, as shown in Fig. 8. From the analysis in Section V-A.3, for a given K^{be}, to satisfy the constraint $\underline{\beta} \le \beta^+$, it is required that $K^b \le K^{b'}$, where $K^{b'}$ is defined in (20). Therefore, we have $\bar{K}^b = \lfloor \max_{K^{be}} K^{b'} \rfloor$. Using the system setup in Fig. 5(a) as an example, Fig. 9 plots $K^{b'}$ versus K^{be}, and $K^{b'}$ achieves a maximum of 431.88 when $K^{be} = 125$. Consequently, $\bar{K}^b = \lfloor 431.88 \rfloor = 431$, which agrees with the result we found using exhaustive search. Similarly, in the example in Fig. 5(c) with $P_{fa} = 10^{-8}$, $K^{b'}$ achieves a maximum of 1246.6 when $K^{be} = 57$. Thus, $\bar{K}^b = \lfloor 1246.6 \rfloor = 1246$, which is the same as the exhaustive search result.

To summarize, given N_b, N_e, and other parameters including θ and γ, to ensure that cooperation can help both SC^b and SC^{be} improve their payoffs, colluders should first ensure that $\underline{K}^{be} \le K^{be} \le \bar{K}^{be}$ and $K^b \le \bar{K}^b$. Then, attackers should further check whether (K^b, K^{be}) satisfies the constraints in (22) and

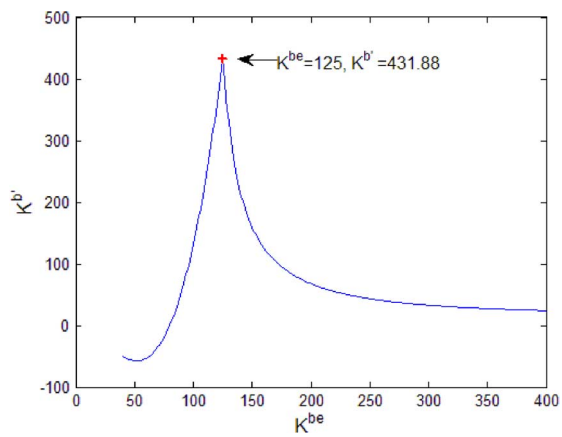


Fig. 9. $K^{b'}$ versus K^{be}. $N_b = N_e = 50\,000$, $\sigma_w^2 = \sigma_n^2 = 1$, $\gamma = 1/3$, $P_{fa} = 10^{-3}$, and $\theta = 50$.

whether $\mathbb{S}_p$ is nonempty. If $(K^b, K^{be}) \in \mathbb{K}_p$, colluders should use (17) and (19) to calculate $\bar{\beta}$ and $\underline{\beta}$, respectively, and find $\mathbb{S}_p = \{(\nu^b, \nu^{be}) : \underline{\beta} \le \beta \le \min(\bar{\beta}, \beta^+)\}$. Compared to the scenario where SC^b and SC^{be} do not cooperate, all colluders increase their payoffs by cooperating and selecting any point in $\mathbb{S}_p$. Moreover, every point in $\mathbb{S}_p$ is Pareto optimal, and any reasonable attacker will agree to go.

B. Collusion Strategies

Given $\mathbb{S}_p$, colluders negotiate with each other and reach an agreement on which pair (ν^b, ν^{be}) in $\mathbb{S}_p$ to select (or equivalently, which β to use during collusion). They select different collusion strategies depending on how they define fairness of collusion. In this section, we will quickly review our prior work in [21] on different fairness constraints and colluder bargaining process.

1) Absolute Fairness: With the absolute fairness criterion, given K^b, K^{be}, N_b, and N_e, colluders seek the $\beta \in [\underline{\beta}, \min(\bar{\beta}, \beta^+)]$ that makes all colluders have the same utility, that is, $\nu^b = \nu^{be}$. Note that even if $\mathbb{S}_p$ is not empty, it is possible that the absolute fairness solution does not exist, that is, there is no pair $(\nu^b, \nu^{be}) \in \mathbb{S}_p$ where $\nu^b = \nu^{be}$. As an example, consider the system setup in Fig. 5(a) where $N_b = N_e = 50\,000$. When $(K^b, K^{be}) = (60, 95)$, following the analysis in Section V-A.2, β should be in the range [0.5308,0.5858], which gives $0.0454 \le \nu^b \le 0.1084$ and $0 \le \nu^{be} \le 0.0390$. In this example, even though $\mathbb{S}_p \neq \emptyset$, $\max(\nu^{be}) < \min(\nu^b)$ and, therefore, the absolute fairness solution does not exist.

To investigate when the absolute fairness solution exists, note that ν^b is a decreasing function of β and ν^{be} is an increasing function of β. Therefore, given $\underline{\beta} \le \beta \le \min(\bar{\beta}, \beta^+)$, we have $\nu^b(\min(\bar{\beta}, \beta^+)) \le \nu^b \le \nu^b(\underline{\beta})$ and $\nu^{be}(\underline{\beta}) \le \nu^{be} \le \nu^{be}(\min(\bar{\beta}, \beta^+))$. The absolute fairness solution exists only if the two intervals, $[\nu^b(\min(\bar{\beta}, \beta^+)), \nu^b(\underline{\beta})]$ and $[\nu^{be}(\underline{\beta}), \nu^{be}(\min(\bar{\beta}, \beta^+))]$, overlap with each other, that is,

$$\nu^{be}(\underline{\beta}) \le \nu^b(\underline{\beta}) \qquad \nu^b\left(\min(\bar{\beta}, \beta^+)\right) \le \nu^{be}\left(\min(\bar{\beta}, \beta^+)\right). \tag{24}$$

If (24) is not satisfied, colluders should consider other fairness criteria other than absolute fairness.

2) MaxSum Fairness: With the MaxSum fairness, colluders look for the β that maximizes the summation of all colluders' utilities, that is, $g_{ms}(\beta) \triangleq K^b\nu^b(\beta) + K^{be}\nu^{be}(\beta)$. To find the MaxSum fairness solution, colluders first find the root of $(\partial g_{ms}(\beta)/\partial\beta) = 0$ and check whether the solutions fall in the range $[\underline{\beta}, \min(\bar{\beta}, \beta^+)]$. If not, they should check the two boundary points $\underline{\beta}$ and $\min(\bar{\beta}, \beta^+)$, and select the one that gives a larger $g_{ms}(\beta)$.

3) Proportional Fairness: With proportional fairness, the Nash Bargaining solution aims to maximize the objective function $g_{nbs}(\beta) \triangleq (\nu^b - \underline{\nu}^b)^{a_b}(\nu^{be} - \underline{\nu}^{be})^{a_{be}}$ where a_b and a_{be} are the bargaining powers of SC^b and SC^{be}, respectively. To find the Nash Bargaining solution, same as in the MaxSum fairness solution, colluders first find the root of $(\partial g_{nbs}/\partial\beta) = 0$ and check if it is in the range $[\underline{\beta}, \min(\bar{\beta}, \beta^+)]$. If not, colluders should check the two boundary points, $\underline{\beta}$ and $\min(\bar{\beta}, \beta^+)$, select the one that gives a larger $g_{nbs}(\beta)$, and use that parameter during collusion.

To illustrate how colluders select different collusion strategies in $\mathbb{S}_p$ based on different fairness criteria, we consider an example where $N_b = N_e = 50\,000$, $K^b = 80$, $K^{be} = 150$, $\theta = 50$, $\gamma = 1/3$, and $P_{fa} = 10^{-3}$. In this example, $\underline{\nu}^b = 0$ and $\underline{\nu}^{be} = \nu^{be}_{nc} = 0.1159$. From (17) and (19), $\underline{\beta} = 0.3071$, $\bar{\beta} = 0.7450 > \beta^+ = 0.5858$. Therefore, $\mathbb{S}_p = \{(\nu^b, \nu^{be}) : 0.3071 \le \beta \le 0.5858\}$.

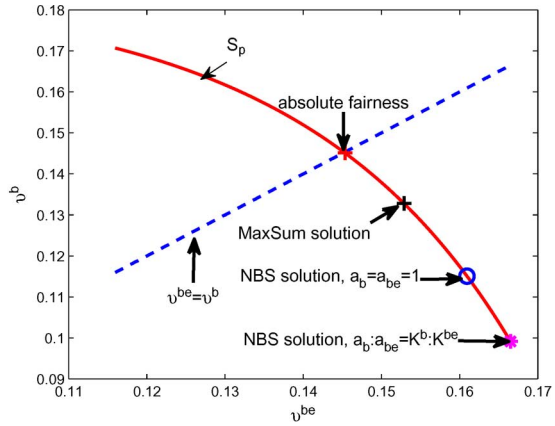


Fig. 10. Example of the bargaining result. $N_b = N_e = 50\,000$, $K^b = 80$, $K^{be} = 150$, $\theta = 50$, and $\gamma = 1/3$. The probability of falsely accusing an innocent user is $P_{fa} = 10^{-3}$.

We first find the absolute fairness solution $(\nu^b_{abs}, \nu^{be}_{abs})$. In the above example, $\nu^{be}(\underline{\beta}) = 0.1159 < \nu^b(\underline{\beta}) = 0.1707$ and $\nu^b(\beta^+) = 0.0992 < \nu^{be}(\beta^+) = 0.1665$. Therefore, the absolute fairness solution exists, and is $\nu^b_{abs} = \nu^{be}_{abs} = 0.1452$ with $\beta_{abs} = 0.4544$. If colluders prefer the MaxSum fairness criterion, we have $\beta_{ms} = 0.4982$ and $(\nu^b_{ms}, \nu^{be}_{ms}) = (0.1328, 0.1529)$. If colluders choose the Nash Bargaining solution with $a_b = a_{be} = 1$, then the solution is $\beta_{nbs,e} = 0.5485$, which gives $(\nu^b_{nbs,e}, \nu^{be}_{nbs,e}) = (0.1151, 0.1609)$. If colluders prefer proportional fairness with $a_b : a_{be} = K^b : K^{be}$, we have $\beta_{nbs,p} = \beta^+ = 0.5858$ and $(\nu^b_{nbs,p}, \nu^{be}_{nbs,p}) = (0.0992, 0.1665)$. Fig. 10 shows $\mathbb{S}_p$ and different bargaining solutions.

C. Maximum Payoff Collusion

Given K^b and K^{be}, Section V-A and V-B analyze how colluders select the collusion parameter β to ensure that cooperation increases all attackers' utilities and how to achieve fair collusion, respectively. During collusion, in addition to β, attackers can also select with whom to collude and the number of fellow colluders, that is, K^b and K^{be}. In this section, we will investigate the impact of (K^b, K^{be}) on colluders' utilities and analyze how attackers choose K^b and K^{be} to maximize their own payoffs.

From Section IV-B, when colluders receive fingerprinted copies of the same resolution, colluding with more people does not always increase an attacker's payoff. This is also true when colluders receive copies of different resolutions. Using SC^{be} as an example, Fig. 11 shows the impact of the number of colluders on ν^{be}. The system setup in Fig. 11 is the same as that in Fig. 5(a), and $K^{be} = 150$ is fixed.

In Fig. 11(a), we consider the scenario where K^{be} is fixed as 150 and colluders select the Nash bargaining solution with $a_b : a_{be} = K^b : K^{be}$. Fig. 11(a) plots ν^{be} when K^b takes different values. As shown in Fig. 11(a), in this example, ν^{be} achieves the maximum of 0.1681 when $K^b = 76$, and it decreases if K^b continues to increase. When $K^b \ge 78$, the optimal β that maximizes $g_{nbs}(\beta)$ with $a_b : a_{be} = K^b : K^{be}$ is the upper bound β^+, and ν^{be} decreases fast as K^b continues to increase. When $K^b > 159$, collaborating with colluders in SC^b does not help SC^{be} further increase their utilities, and colluders

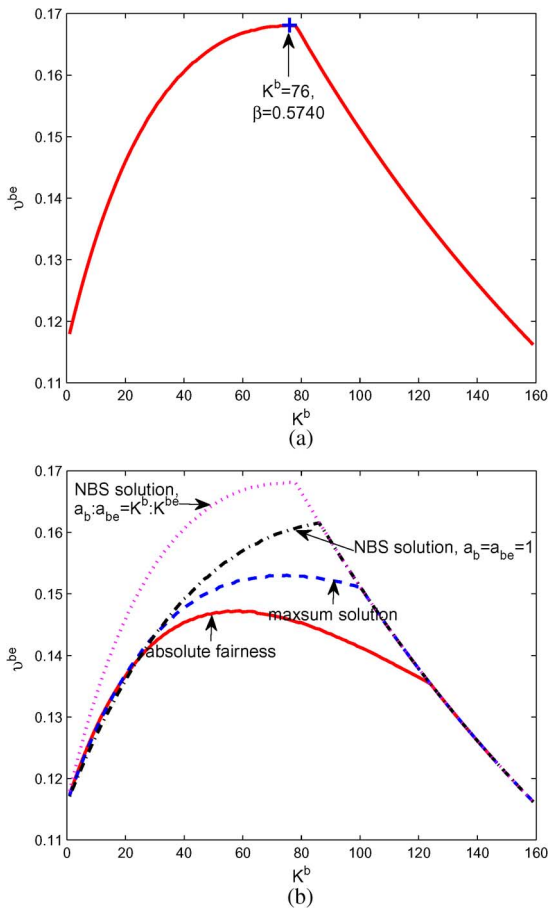


Fig. 11. ν^{be} when $K^{be} = 150$ is fixed. $N_b = N_e = 50\,000$, $\sigma_w^2 = \sigma_n^2 = 1$, $\gamma = 1/3$, $P_{fa} = 10^{-3}$, and $\theta = 50$. (a) Nash bargaining solution with $a_b : a_{be} = K^b : K^{be}$. (b) Comparison of the absolute fairness solution, the maxsum solution, and the Nash bargaining solutions.

will only collude with their fellow attackers in the same subgroup. Fig. 11(b) compares ν^{be} when colluders select different collusion strategies including the absolute fairness solution, the MaxSum solution, and the Nash bargaining solutions. It shows that, in this example, colluders in SC^{be} receive the highest payoffs from collusion if they choose the Nash bargaining solution with $a_b : a_{be} = K^b : K^{be}$. To conclude, from Fig. 11(b), with a fixed $K^{be} = 150$, if colluders in SC^{be} want to maximize their own payoffs, the best strategy is to find another 76 attackers who receive the low resolution copy and to choose the Nash bargaining solution with $a_b : a_{be} = K^b : K^{be}$.

In the example in Fig. 11, we fix $K^{be} = 150$ and find the optimum K^b to maximize SC^{be}'s utility. In practice, a colluder may wish to select both K^{be} and K^b to maximize his or her payoff. As an example, Fig. 12 plots υ^{be} when K^b and K^{be} take different values and when colluders use the Nash Bargaining solution with $a^b : a^{be} = K^b : K^{be}$. The system setup is the same as in Fig. 11(a). In this example, υ^{be} achieves the maximum 0.1742 when $(K^b = 52, K^{be} = 176)$, and a colluder with a high-resolution copy should find 52 colluders with low-resolution copies and another 175 colluders with high-resolution copies to maximize his/her payoff.

When attackers choose the absolute fairness solution, a colluder in SC^{be} is interested to find the K^{b*} and K^{be^*} that maximize $\nu_{abs} = \nu_{abs}^b = \nu_{abs}^{be}$, where $(\nu_{abs}^b, \nu_{abs}^{be})$ is the absolute

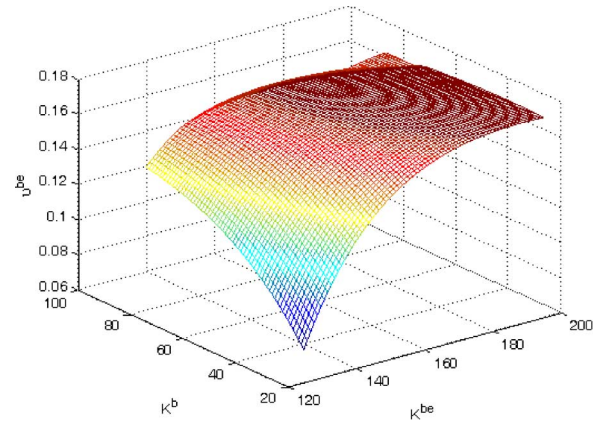


Fig. 12. Maximization of υ^{be} with the Nash Bargaining solution where $a^b : a^{be} = K^b : K^{be}$. $N_b = N_e = 50\,000$, $\theta = 50$, and $\gamma = 1/3$. The probability of falsely accusing an innocent user is $P_{fa} = 10^{-3}$.

fairness solution in Section V-B. Similarly, if colluders prefer the MaxSum fairness solution, a colluder in SC^{be} is interested in the pair (K^{b*}, K^{be*}) that maximizes his or her payoff, that is, $(K^{b*}, K^{be*}) = \arg\max_{(K^b, K^{be}) \in \mathbb{K}_p} \nu_{ms}^{be}$ where $(\nu_{ms}^b, \nu_{ms}^{be})$ is the MaxSum solution in Section V-B. When colluders choose the Nash bargaining solution, a colluder in SC^{be} would like to find the optimal (K^{b*}, K^{be*}) that maximizes his or her payoff, that is, $(K^{b*}, K^{be*}) = \arg\max_{(K^b, K^{be}) \in \mathbb{K}_p} \nu_{nbs}^{be}$ where $(\nu_{nbs}^b, \nu_{nbs}^{be})$ is the Nash bargaining solution in Section V-B.

We find the above solutions for the example in Fig. 5(a), and the results are shown in Table II. As an example, from Table II, if colluders prefer the MaxSum fairness solution, then for a colluder in SC^{be} to maximize his or her own payoff, he/she should find another 205 attackers who also receive high resolution copies and 16 attackers who have the base layer only. If we compare the four solutions in Table II, to maximize ν^{be}, the optimal collusion strategy for a colluder in SC^{be} is to let $(K^b, K^{be}) = (52, 176)$ and to select the Nash Bargaining solution with $a_b : a_{be} = K^b : K^{be}$. It helps colluders in SC^{be} receive a maximum payoff of 0.1742 among all possible ν^{be}s that they could have.

For colluder $i \in SC^b$, we can use the same method to find the optimum pair (K^b, K^{be}) that maximizes $u^{(i)}$'s utility ν^b, and Table III shows the results. For instance, from Table III, if colluders decide to select the Nash bargaining solution with $a_b : a_{be} = K^b : K^{be}$, then to maximize ν^b, a colluder in SC^b should find additional 105 attackers who receive the base layer only and another 97 attackers who have the high resolution copies. Similarly, by comparing all four collusion strategies, if colluder $i \in SC^b$ hopes to maximize his or her payoff, $u^{(i)}$ should let $(K^b, K^{be}) = (1, 126)$ (that is, find another 126 attackers who receive both layers but no more attackers who have the base layer only) and select the Nash bargaining solution with $a_b = a_{be} = 1$. By doing so, ν^b achieves the maximum of 0.2047.

VI. Simulation Results

In our simulations, we test on the first 40 frames of the "carphone" sequence in QCIF format, which is a popular test sequence for video processing. We observe the same trend for other video sequences. The base layer includes all the odd frames, and the enhancement layer contains all the even frames. The length of the fingerprints embedded in each frame is 2500,

TABLE II
MAXIMIZATION OF ν^{be}. $N_b = N_e = 50\,000$, $\theta = 50$, $\gamma = 1/3$, AND $P_{fa} = 10^{-3}$

Fairness criteria	K^{b*}	K^{be*}	β^*	ν^{be*}
Absolute fairness	1	182	0.0062	0.1624
MaxSum fairness	16	206	0.1274	0.1682
Proportional fairness, $a_b = a_{be} = 1$	46	188	0.3792	0.1707
Proportional fairness, $a_b : a_{be} = K^b : K^{be}$	52	176	0.4421	**0.1742**

TABLE III
MAXIMIZATION OF ν^b.$N_b = N_e = 50\,000$, $\theta = 50$, $\gamma = 1/3$, AND $P_{fa} = 10^{-3}$

Fairness criteria	K^{b*}	K^{be*}	β^*	ν^{b*}
Absolute fairness	1	182	0.0062	0.1624
MaxSum fairness	106	97	0.5858	0.1803
Proportional fairness, $a_b = a_{be} = 1$	1	126	0.0076	**0.2074**
Proportional fairness, $a_b : a_{be} = K^b : K^{be}$	106	97	0.5858	0.1803

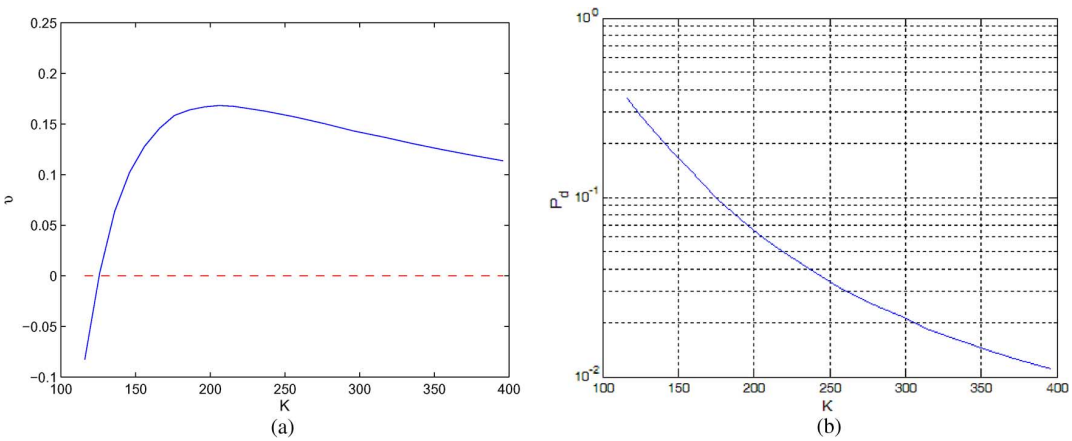


Fig. 13. Simulation results when all attackers receive fingerprinted copies of high resolution. The system setup is the same as that in Fig. 1(a). $\theta = 50$, $\gamma = 1/3$, and $P_{fa} = 10^{-3}$. The results are based on 2000 simulation runs. (a) ν. (b) P_d.

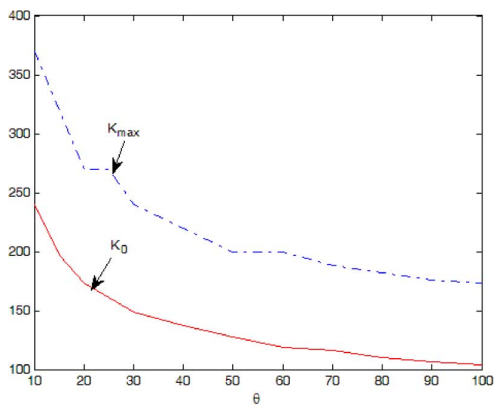


Fig. 14. Simulation results of K_0 and $K_{\max}$ when all attackers receive fingerprinted copies of high resolution. The system setup is the same as that in Fig. 1(a) with $\gamma = 1/3$ and $P_{fa} = 10^{-3}$, and θ varies from 10 to 100.

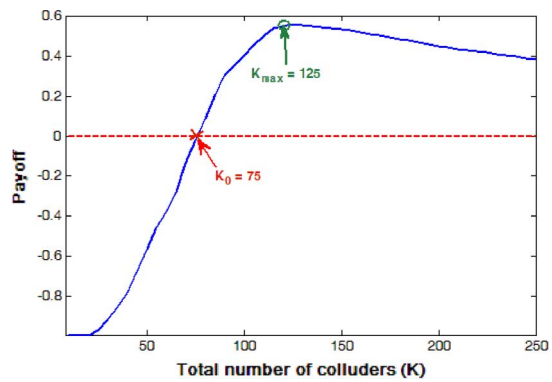


Fig. 15. $\nu^{(i)}$ when the host signal is 256 × 256 Lena image with $P_{fa} = 10^{-3}$, $\sigma_n^2 = \sigma_w^2$, $N = 65\,536$, and $\theta = 100$.

and the lengths of the fingerprints embedded in the base layer and the enhancement layer are $N_b = 50\,000$ and $N_e = 50\,000$, respectively. We use orthogonal fingerprint modulation [16], and use spread spectrum embedding [24] to embed fingerprints into the host signals. During collusion, colluders follow the two-stage collusion in Section II-A-2, and they adjust the power of the additive noise such that $\|\mathbf{n}_j\|^2 = \|JND_j\mathbf{W}_j^{(i)}\|^2$. In addition, as an example, when defining the utility function, we let colluders select $\theta = 50$ and $\gamma = 1/3$. When identifying colluders, the fingerprint detector follows Section II-B and uses the self-probing detector in [22]. The fingerprint detector selects the threshold h such that the probability of falsely accusing an innocent is $P_{fa} = 10^{-3}$.

We first consider the scenario where all colluders receive the high resolution copies. In such a scenario, they simply average all the fingerprinted copies that they have and then add additive noise to further hinder the detection. The simulation results of the colluders' utilities are shown in Fig. 13(a), and it

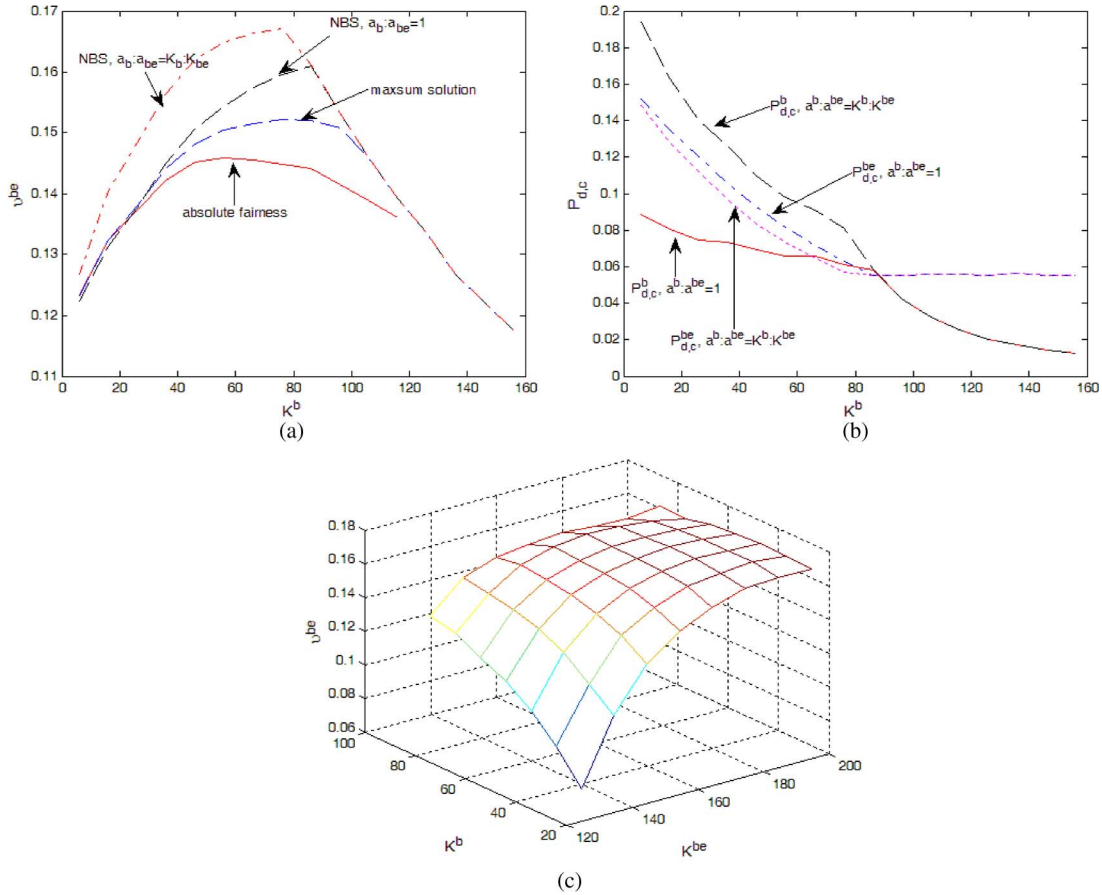


Fig. 16. Simulation results of ν^{be} when colluders receive fingerprinted copies of different resolutions. The system setup is the same as that in Fig. 11(a). The results are based on 2000 simulation runs. (a) υ^{be}. $K^{be} = 150$. (b) $P_{d,c}$ with NBS and $K^{be} = 150$. (c) υ^{be}_{nbs} with $a^b : a^{be} = K^b : K^{be}$.

is consistent with our analysis results shown in Fig. 1(a). A colluder receives a positive payoff when there are more than 125 colluders, and ν reaches the maximum when K is around 206. As K continues to increase, ν starts decreasing. Fig. 13(b) plots the corresponding P_d. From Fig. 13, although a larger K always decreases a colluder's risk, it does not always increase a colluder's utility when the reward received from collusion is also considered.

Fig. 14 shows the simulated K_0 and $K_{\max}$, where we use our simulation results to find the smallest K that makes $\nu > 0$ and the K that maximizes ν, respectively, when θ varies. It is consistent with our analytical results in Figs. 2(a) and 3(a), and both K_0 and $K_{\max}$ decrease as θ increases.

When colluders use different post-collusion processing techniques, colluders may have different probability of being detected and thus different utilities, but we will observe the same trend as in Figs. 1 and 13(a). As an example, Fig. 15 plots colluders' utility when a 3×3 Gaussian low pass filter with variance 0.4 is applied after averaging collusion. The host signal is 256×256 Lena, and spread spectrum embedding is used. Fig. 15 is based on 200 simulation runs. We observe the same trend for other parameter values and other post-collusion processing. Figs. 1 and 15 show the same trend, and colluders can use the same strategy to study when to collude and find the optimal size of coalition.

We then consider the scenario where colluders receive fingerprinted copies of different resolutions. Following the example in Fig. 11(a), we fix the number of colluders who receive high resolution copies as $K^{be} = 150$. We select K^b such that $(K^b, K^{be} = 150) \in \mathbb{K}_p$ and it is possible for colluders to find at least one β that increases all colluders' payoffs. Fig. 16(a) shows the simulation results of ν^{be} with the absolute fairness, the maxsum solution, the Nash bargaining solutions with $a_b : a_{be} = 1$ and $a_b : a_{be} = K^b : K^{be}$, respectively, and Fig. 16(b) plots the corresponding colluders' risk of being detected when they use the Nash Bargaining solutions. They are consistent with our analytical results shown in Fig. 11. In Fig. 16, ν^{be} of the NBS with $a_b : a_{be} = K^b : K^{be}$ reaches the maximum when $K^b = 76$, which gives the same result as in Fig. 11(a). In addition, for NBS with $a_b : a_{be} = K^b : K^{be}$, when $K^b > 78$ and $\beta = \beta^+$ is used, $P^{be}_{d,c}$ remains the same as K^b increases, which causes the fast decrease of ν^{be}. For NBS with $a^b : a^{be} = 1$, we observe the same trend when $K^b > 86$ and colluders select $\beta = \beta^+$ to maximize g_{nbs}. Comparing the two Nash Bargaining solutions in Fig. 16, using the bargaining powers $a^b : a^{be} = K^b : K^{be}$ helps colluders in SC^{be} gain a better position in the bargaining process since $K^{be} > K^b$ in Fig. 16, lowers their probability of detected and increases their utilities. It shows that the Nash Bargaining solution favors the player with a larger bargaining power by awarding him/her a higher utility. Fig. 16(c) plots ν^{be} of the NBS with $a_b : a_{be} = K^b : K^{be}$. From Fig. 16(c), ν^{be} achieves the maximum 0.1739 when $(K^b = 52, K^{be} = 176)$, and this is consistent with our analytical results in Fig. 12 and Table II.

VII. Conclusions

This paper provides a case study of cooperation analysis for multiuser collusion in multimedia fingerprinting. In this paper, we build a game-theoretic framework to analyze the necessary conditions for attackers to cooperate with each other, examine the impact of the selection of fellow attackers on an attacker's payoff, and investigate the optimum strategies for colluders to find their fellow attackers in order to maximize their own utilities.

We first consider a scenario where all colluders receive fingerprinted copies of the same resolution and the colluded copy is a simple average of all copies with equal weights. In such a scenario, we first investigate K_0, the smallest number of colluders that gives attackers a non-negative payoff. Attackers collude with each other if and only if the total number of colluders is larger than or equal to K_0. We then show that colluding with more attackers does not always increase a colluder's payoff, and analyze the optimum number of colluders $(K_{\max})$ that maximizes a colluder's utility.

We then consider the scenario where attackers receive fingerprinted copies of different resolutions. Our analysis shows that in this scenario, colluding with more attackers does not always increase an attacker's payoff and attackers may not always want to cooperate with each other. They collude with each other if and only if cooperation helps increase all attackers' utilities. We first investigate the necessary conditions for colluders to cooperate with each other. We analyze $\mathbb{K}_p$, the set including all pairs of (K^b, K^{be}) where it is possible for all colluders to benefit from cooperation, and explore all possible collusion strategies that increase every attacker's utility for a given $(K^b, K^{be}) \in \mathbb{K}_p$. We then examine how the number of colluders in each subgroup, (K^b, K^{be}), affects colluders' utilities, and analyze the optimum strategy to select fellow attackers if a colluder wants to maximize his/her own payoff.

Our contribution is twofold. From colluder perspective, our work shows that cooperation does not always increase a colluder's payoff, and colluders cooperate with each other if and only if cooperation benefits all colluders. Our work provides a framework for a colluder to determine when to participate in collusion and how to select his/her fellow attackers to maximize his/her own payoff. From traitor tracing perspective, for the high-risk high-return scenarios considered in our work, the proposed framework enables the digital rights enforcer to estimate the likely colluder group size, and design collusion-resistant fingerprinting systems accordingly. Our analysis of the colluder coalition formation game can also be extended to study coalition formation and partner selection in other social networks and other applications.

References

[1] X. Cheng, C. Dale, and J. Liu, "Statistics and social networking of YouTube videos," in *Proc. IEEE Int. Workshop Quality of Service (IWQoS)*, Jun. 2008, pp. 229–238.

[2] G. P. Gummadi, R. J. Dunn, S. Saroiu, S. D. Gribble, H. M. Levy, and J. Zahorjan, "Measurement, modeling and analysis of a peer-to-peer file-sharing workload," in *Proc. 19th ACM Symp. Oper. Syst. Principles (SOSP-19)*, Oct. 2003, pp. 314–329.

[3] C. Lee, "IPTV over next generation networks in ITU-U," in *Proc. IEEE/IFIP 2nd Int. Workshop Broadband Convergence Netw.*, May 2007, pp. 1–18.

[4] X. Hei, Y. Liu, and K. W. Ross, "IPTV over P2P streaming networks: The mesh-pull approach," *IEEE Commun. Mag.*, vol. 46, no. 2, pp. 86–92, Feb. 2008.

[5] E. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim, "A survey and comparison of peer-to-peer overlay network schemes," *IEEE Commun. Surveys Tutorial*, vol. 7, no. 2, pp. 72–93, Mar. 2004.

[6] B. Wellman and S. D. Berkowitz, *Social Structures: A Network Approach*. Cambridge, U.K.: Cambridge Univ. Press, 1988.

[7] W. Saad, Z. Han, M. Debbah, and A. Hjrungnes, "Distributed merge and split algorithm for fair cooperation in wireless networks," in *IEEE Int. Conf. Commun., Workshop Cooperative Commun. Netw.*, May 2008, pp. 311–315.

[8] W. Saad, Z. Han, M. Debbah, A. Hjrungnes, and T. Basar, "Coalitional games for distributed collaborative spectrum sensing in cognitive radio networks," *Proc. IEEE INFOCOM*, pp. 2114–2122, Apr. 2009.

[9] D. Knoke and S. Yang, *Social Network Analysis*, 2nd ed. Thousand Oaks, CA: SAGE, 2008.

[10] S. Fortunato, "Community detection in graphs," *Physics Rep.*, vol. 486, no. 3–5, pp. 75–174, Feb. 2010.

[11] International Intellectual Property Alliance, "Cover letter to U.S. trade representatives," Feb. 18, 2010 [Online]. Available: http://www.iipa.com/rbc/2010/2010SPEC301COVERLETTER.pdf

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

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

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

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

[16] Z. J. Wang, M. Wu, H. V. 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.

[17] F. Ergun, J. Killian, and R. Kumar, "A note on the limits of collusion-resistant watermarks," *Adv. Cryptology EuroCrypto 99, Lecture Notes Comput. Sci.*, vol. 1592, pp. 140–149, 2001.

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

[19] D. Kirovski and M. K. Mihcak, "Bounded Gaussian fingerprints and the gradient collusion attack," in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Process.*, Mar. 2005, vol. II, pp. 1037–1040.

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

[21] W. S. Lin, H. V. Zhao, and K. J. R. Liu, "Game-theoretic strategies and equilibriums in multimedia fingerprinting social networks," *IEEE Trans. Multimedia*, vol. 13, no. 2, pp. 191–205, Apr. 2011.

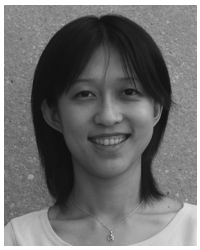
[22] W. S. Lin, H. V. Zhao, and K. J. R. Liu, "Behavior forensics with side information for multimedia fingerprinting social networks," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 911–927, Dec. 2009.

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

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

[25] G. Tardos, "Optimal probabilistic fingerprint codes," in *Proc. 35th Annu. ACM Symp. Theory Comput.*, 2003, pp. 116–125.

[26] B. Skoric, S. Katzenbeisser, and M. U. Celik, "Symmetric Tardos fingerprinting codes for arbitrary alphabet sizes," *Designs, Codes and Cryptography*, vol. 46, no. 2, pp. 137–166, 2008.



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 at 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 at 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. She is a coauthor of "Multimedia Fingerprinting Forensics for Traitor Tracing" (Hindawi, 2005) and "Behavior Dynamics in Media-Sharing Social Networks" (Cambridge University Press, 2011). Her research interests include media-sharing social networks, information security and forensics, digital communications, and signal processing.

Dr. Zhao is the Associate Editor for the IEEE SIGNAL PROCESSING LETTERS and *Elsevier Journal of Visual Communication and Image Representation*, and a Guest Editor of special issue on Signal and Information Processing for Social Learning and Networking of IEEE SIGNAL PROCESSING MAGAZINE. She was the recipient of the IEEE Signal Processing Society (SPS) 2008 Young Author Best Paper Award.

W. Sabrina Lin (M'06) received the B.S. and M.S. degrees in electrical engineering from the National Taiwan University, Taipei, Taiwan, in 2002 and 2004, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Maryland at College Park in 2009.

She coauthored the book "Behavior Dynamics in Media-Sharing Social Networks" (Cambridge University Press, 2011). Her research interests are in the area of information security and forensics, multimedia signal processing and multimedia social network analysis.

Dr. Lin was the recipient of the University of Maryland Innovation Award in 2011.

K. J. Ray Liu (F'03) is Christine Kim Eminent Professor of Information Technology at the University of Maryland at College Park. He leads the Maryland Signals and Information Group conducting research encompassing broad areas of signal processing and communications with recent focus on cooperative communications, cognitive networking, social learning and networks, and information forensics and security.

Dr. Liu is an ISI Highly-Cited Author in Computer Science and a Fellow of the AAAS. He is President of IEEE Signal Processing Society where he has served as Vice President-Publications and Board of Governor. He was the Editor-in-Chief of the IEEE SIGNAL PROCESSING MAGAZINE and the founding Editor-in-Chief of the *EURASIP Journal on Advances in Signal Processing*. He was named a Distinguished Scholar-Teacher of the University of Maryland at College Park in 2007. He was the recipient of numerous honors and awards including the IEEE Signal Processing Society Technical Achievement Award and Distinguished Lecturer. He also received various teaching and research recognitions from the University of Maryland, including the university-level Invention of the Year Award, and the Poole and Kent Senior Faculty Teaching Award and Outstanding Faculty Research Award, both from A. James Clark School of Engineering.