MULTI-USER COLLUSION BEHAVIOR FORENSICS: GAME THEORETIC FORMULATION OF FAIRNESS DYNAMICS

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

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

ABSTRACT

Multi-user collusion is an cost-effective attack against digital fingerprinting, in which a group of attackers collectively undermine the traitor tracing capability of digital fingerprints. However, during multi-user collusion, each colluder wishes to minimize his/her own risk and maximize his/her own profit, and different colluders have different objectives. Thus, an important issue during collusion is to agree on how to distribute the risk/profit among colluders and ensure fairness of the attack. To have a better understanding of the attackers' behavior during collusion to achieve fairness, this paper models the dynamics among colluders as a non-cooperative game. We then study the Pareto-Optimal set, where no colluder can further increase his/her own payoff without decreasing others', and analyze the Nash Bargaining solution of this game.

Index Terms— Multimedia forensics, security, game theory

1. INTRODUCTION

Digital fingerprinting is an emerging forensic tool to protect multimedia from illegal usage and unauthorized redistribution. It embeds a unique label, known as fingerprint, into every distributed copy to track the usage of multimedia data. In digital fingerprinting systems, there is a powerful attack called multi-user collusion, where a group of attackers work together to effectively remove the identifying fingerprints. To design anti-collusion fingerprints and provide trustworthy traitor tracing performance, it is important to study collusion attacks and understand the challenges in multimedia forensics. There is a lot of work in the literature exploring different types of collusion attacks and analyzing their effectiveness [1, 2, 3].

Colluders have to collaborate with each other during collusion to reduce their chance of being caught. However, different colluders have different objectives, and every colluder wishes to minimize his/her risk . To address this conflict, colluders have to agree on how to distribute the risk and achieve "fairness" of the attack. It raises complicated dynamics among colluders to ensure fairness of collusion, and it is important to formulate this dynamics, understand colluders' behavior during collusion, and analyze its impact on the traitor tracing performance of multimedia fingerprints.

In this paper, we propose a game-theoretic frame work to formulate and analyze this complex colluder dynamics. We model the dynamics among colluders as a non-cooperative game where each colluder tries to maximize his/her individual payoff under the fairness constraint. We calculate the Pareto Optimal set of this game, where no colluder can further increase his/her own payoff without decreasing others'. We also consider different definitions of "fairness", investigate how the colluders would like to share the risk and the profit, and study the Nash Bargaining solution.

The rest of the paper is as follows. Section 2 introduces the multimedia fingerprinting systems that we consider in this paper, and formulates the fairness dynamics among colluders. Section 3 derives the Pareto-Optimal set and the Nash bargaining solution of this game. We show simulation results in Section 4, and conclusions are drawn in Section 5.

2. SYSTEM MODEL

2.1. Scalable Video Coding Systems

Nowadays, scalable video coding is widely adopted to accommodate heterogenous networks and devices with different storage and computing capability. It decomposes the video sequence into different 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. Without loss of generality, we consider a two-layer temporally scalable video coding system, where different frames are encoded at different layers [4]. Take MPEG-2 video coding as an example, the base layer includes all the I frames, and the enhancement layer may contain all the P and B frames.

Define F_b and F_e as the sets containing the indices of the frames that are encoded in the base layer and the enhancement layer, respectively; and let $F^{(i)}$ be the set that contains the indices of the frames that user $\mathbf{u}^{(i)}$ receives. U^b is the subgroup of users who receive the base layer only; and $U^{b,e}$ contains all users who subscribe to the high quality version containing both layers.

2.2. Scalable Multimedia Fingerprinting System

Fingerprint Embedding We use the spread spectrum embedding [5, 6] to embed fingerprints in the host signal. Let $\mathbf{S}_j$ be the jth frame in the video, and for each user $\mathbf{u}^{(i)}$ who subscribes to frame j, the content owner generates a unique fingerprint $\mathbf{W}_j^{(i)}$, with the same length as $\mathbf{S}_j$. The fingerprinted frame is $\mathbf{X}_j^{(i)} = \mathbf{S}_j + JND_j \mathbf{W}_j^{(i)}$, which is distributed to $\mathbf{u}^{(i)}$. JND [6] here is used to control the energy of the embedded fingerprints and make the fingerprinted copy be perceptually the same as the original one. In this paper, we first generate independent vector from Gaussian distribution $\mathcal{N}(0, \sigma_w^2)$, and then apply Gram-Schmidt orthogonalization to generate orthogonal fingerprints for different users.

Multi-user Collusion In this paper, we only consider averaging based collusion because nonlinear collusion can be modelled as averaging collusion with additive noise [7], and all collusion attacks have similar performance with colluded copies of the same quality.

During collusion, depending on the resolutions of their received copies, the colluders are divided into two non-overlapping subgroups. SC^b is the set including the indices of the colluders who receive the base layer only and $SC^{b,e}$ contains the indices of the colluders who

The authors can be reached at wylin@eng.umd.edu, vzhao@ece.ualberta.ca, and kjrliu@eng.umd.edu.

1-4244-1437-7/07/$20.00 ©2007 IEEE

subscribe to the high quality version. K^b and $K^{b,e}$ are the number of colluders in SC^b and $SC^{b,e}$, respectively, and $K = K^b + K^{b,e}$ is the total number of colluders.

In this paper, we consider the scenario where colluders who receive fingerprinted copies of the same resolution agree to share the same risk. Following the work in [4], colluders apply intra-group collusion first: for each frame $j \in F_b$ that they receive, colluders in SC^b generate $\mathbf{Z}_j^b = \sum_{k \in SC^b} \mathbf{X}_j^{(k)}/K^b$, and for each received frame $j \in F_b \cup F_e$, colluders in $SC^{b,e}$ calculate $\mathbf{Z}_j^{b,e} = \sum_{k \in SC^{b,e}} \mathbf{X}_j^{(k)}/K^{b,e}$. Then, the colluders apply inter-group collusion: for each frame $j \in F_b$ in the base layer, colluders generate $\mathbf{V}_j = \beta \mathbf{Z}_j^b + (1-\beta)\mathbf{Z}_j^{b,e} + \mathbf{n}_j$ where $0 \leq \beta \leq 1$; and for each frame $j \in F_e$ in the enhancement layer, $\mathbf{V}_j = \mathbf{Z}_j^{b,e} + \mathbf{n}_j$. $\mathbf{n}_j$ is the additive noise to further deter the detection performance.

Fingerprint Detection When identifying colluders, the fingerprint detector first extracts the fingerprint $\mathbf{Y}_j$ from frame j in the colluded copy. Then, for each user $\mathbf{u}^{(i)}$, the fingerprint detector calculates the detection statistics

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

compares with a threshold h, and outputs the estimated colluder set $\widehat{SC} = \{i : TN^{(i)} > h\}$. When identifying colluders, the fingerprint detector can use fingerprints extracted from all layers collectively. The fingerprint detector can also examine each individual layer to determine whether a user is involved in collusion. For example, for user $i \in \mathbf{U}^{b,e}$, $\check{F}^{(i)}$ has three choices, $F_b \cup F_e$, F_b and F_e.

Different detection statistics have different means, and the one with the largest mean has the best detection performance. The work in [8] proposed to estimate the means of different detection statistics first, and then use the one with the largest estimated mean when identifying colluders. It was shown that information about the detection statistics' means helps significantly improve the detection performance; and the proposed self-probing fingerprint detector has approximately the same performance as the optimum one, which has perfect knowledge of the means and always select the detection statistics with the best performance.

2.3. Fairness Dynamics among Colluders

During collusion, every colluder wants to minimize his/her own risk and maximizes his/her own profit. Colluders have conflicting objectives and, therefore, an important issue during collusion is to achieve "fairness" of the attack. Absolute fairness is one of the popular models used in the literature, where all colluders share the same risk and have equal probability of being detected. Colluders can also use other definitions of fairness, e.g., proportional fairness, where some colluders benefits more from collusion at a cost of higher risk. We model this dynamics among colluder to achieve "fair" collusion as a game: colluders first define the payoff function (or the utility function) and agree on the "fair" distribution of the risk and the profit. Then, they adjust the collusion parameters (β in the collusion model in Section 2.2) to achieve fairness of collusion.

Colluders wish to minimize their risk of being detected. In addition, when when the colluded copy has higher resolution and better quality, colluders can redistribute the colluded copy with a higher price and thus receive higher profit. Consequently, $\pi^{(i)}$ is a monotonically increasing function of the colluded copy's resolution. Furthermore, colluding with more attackers reduces $\mathbf{u}^{(i)}$'s probability of being detected; while it also reduces the profit that $\mathbf{u}^{(i)}$ receives from the illegal redistribution of multimedia since he/she has to share it with more people.

To address all the above issues, in this paper, we define colluder $\mathbf{u}^{(i)}$'s payoff function as

$$\pi^{(i)} = \frac{\left(1 - P_d^{(i)}\right)^{\gamma_1} F^{\gamma_2}}{K}, \quad (2)$$

Where P_d is $\mathbf{u}^{(i)}$'s risk, and F is the number of frames (or equivalently, the temporal resolution) of the final colluded copy. γ_1, γ_2 are non-negative real numbers that can be adjusted by the colluders to balance the tradeoff among the risk and the profit. Without loss of generality, we use $\gamma_1 = 4, \gamma_2 = 1$ as an example in this paper, and the analysis when using other parameters is the same.

During collusion, every colluder in the game aims to maximize their own payoff $\pi^{(i)}$ and, therefore, there exist conflicting objectives among colluders during collusion. Thus, in our model of the dynamics, colluders maximize their individual payoff function under the fairness constraint. In the collusion model in Section 2.2, we consider the scenario where colluders who receive fingerprinted copies of the same quality agree to share the same payoff. From the definition of the payoff function in (2), having the same payoff is equivalent to sharing the same risk, i.e., $P_d^{(i)} = P_d^{(j)}$ if both colluder i and colluder j receive the low (or high) resolution copies.

3. GAME BETWEEN COLLUDERS

In this section, we will first find the feasible set of the game, and search for the Pareto optimal points, assuming that colluders who receive copies of the same quality agree to share the same risk. Then, we will analyze the Nash-Bargaining solution of the game.

3.1. Feasible Set

Given a N-person general-sum game, there is a certain subset S of R_N, called the feasible set. It is feasible in the sense that, given any $(\pi_1, \pi_2, ..., \pi_N) \in S$, it is possible for the players, acting together, to obtain the utilities $\pi_1, \pi_2, ..., \pi_N$, respectively.

The proposed self-probing fingerprint detector in [8] has approximately the same performance as the optimal detector. Therefore, colluders should consider the worse-case scenario and assume that the fingerprint detector can always select the detection statistics with the largest mean. Following the analysis in [8], under the assumption that the detection noise are i.i.d. Gaussian $\mathcal{N}(0, \sigma_n^2)$,

$$\begin{aligned} P_d^{(i)} &= Q\left(\frac{h - \mu_{max}^{(i)}}{\sigma_n}\right), \\ \mu_{max}^{(i)} &= \mu_b \overset{\triangle}{=} \frac{\beta\sqrt{N_b}}{K^b}\sigma_w \quad \text{for } i \in SC^b, \\ \text{and} \quad \mu_{max}^{(i)} &= \mu_{b,e} \overset{\triangle}{=} \max\{\mu_{b,e}^b, \mu_{b,e}^e, \mu_{b,e}^c\} \quad \text{for } i \in SC^{b,e}, \\ \text{where} \quad \mu_{b,e}^b &= \frac{(1-\beta)\sqrt{N_b}}{K^{b,e}}\sigma_w, \ \mu_{b,e}^e = \frac{\sqrt{N_e}}{K^{b,e}}, \\ \text{and} \quad \mu_{b,e}^c &= \frac{(1-\beta)N_b + N_e}{K^{b,e}\sqrt{N_b + N_e}}\sigma_w. \qquad (3) \end{aligned}$$

$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{\frac{-t^2}{2}} dt$ is the Gaussian tail function.

From (3), for a given β, μ_b is fixed while $\mu_{b,e1}$ may take three different values. To find the feasible set of the game, we need to find the relationship between β and $\mu^{b,e}$ first.

Scenario 1 $\mu_{b,e} = \mu_{b,e}^b$: $\mu_{b,e} = \mu_{b,e}^b$ if and only if $\mu_{b,e}^b \geq \mu_{b,e}^e$, and $\mu_{b,e}^b \geq \mu_{b,e}^c$. So, from (3),

$$(1-\beta) \geq \max\left\{ \frac{\sqrt{N_e}}{\sqrt{N_b}}, \frac{N_e}{\sqrt{N_b}(\sqrt{N_b + N_e} - \sqrt{N_b})} \right\} \quad (4)$$

Note that $\sqrt{N_b}+\sqrt{N_{b,e}} \geq \sqrt{N_b+N_e}$. So the second upper bound in (4) is always larger or equal to the first one. Thus, we have

$$\mu_{b,e} = \mu_{b,e}^b \Leftrightarrow 0 \leq \beta \leq 1 - \frac{N_e}{\sqrt{N_b}(\sqrt{N_b+N_e}-\sqrt{N_b})}. \quad (5)$$

However, for all $N_b > 0$ and $N_e > 0$, the upper bound of β in (5) is always smaller than 0. Therefore, $\mu_{b,e} \neq \mu_{b,e}^b$ and $\mu_{b,e}^b$ cannot be the largest among the three $\mu_{b,e}^b$, $\mu_{b,e}^e$ and $\mu_{b,e}^c$.

Scenario 2 $\mu_{b,e} = \mu_{b,e}^e$: $\mu_{b,e} = \mu_{b,e}^e$ if and only if $\mu_{b,e}^e \geq \mu_{b,e}^b$ and $\mu_{b,e}^e \geq \mu_{b,e}^c$. Therefore, from (3),

$$(1-\beta) \leq \min\left\{\frac{\sqrt{N_e}}{\sqrt{N_b}}, \frac{\sqrt{N_e}(\sqrt{N_b+N_e}-\sqrt{N_e})}{N_b}\right\}. \quad (6)$$

Using the same analysis as in (3), the necessary and sufficient condition for scenario 2 is:

$$\mu_{b,e} = \mu_{b,e}^e \Leftrightarrow 1 - \frac{\sqrt{N_e}(\sqrt{N_b+N_e}-\sqrt{N_e})}{N_b} \leq \beta \leq 1. \quad (7)$$

Scenario 3 $\mu_{b,e} = \mu_{b,e}^c$: Following the same analysis, we can get the necessary and sufficient condition for Scenario 3, which is:

$$\mu_{b,e} = \mu_{b,e}^c \Leftrightarrow 0 \leq \beta \leq 1 - \frac{\sqrt{N_e}(\sqrt{N_b+N_e}-\sqrt{N_e})}{N_b}. \quad (8)$$

From the above analysis on $P_d^{(i)}$, we can calculate the payoffs $\pi^{(i)}$ for all colluders for any given β. From the definition of the payoff function (2), colluders who receive fingerprinted copies of the same quality have the same payoff. We define $\pi_{b,e}$ as the payoff for colluders in $SC^{b,e}$, and π_b as the payoff for colluders in SC^b. Figure 1 plots π_b versus $\pi_{b,e}$, and shows the feasible set R_N which is the solid line.

3.2. Pareto Optimality

After finding the feasible set, it is important to find the set of Pareto-Optimal points. A solution is Pareto-Optimal if and only if no player in the game can increase his/her payoff without decreasing others'. In a bargaining situation, players would always like to settle at a pareto optimal outcome. This is because if they select a point that is not pareto optimal, then there exists another solution where at least one player can have larger payoff without hurting the interest of the other players. Pareto optimal solutions are not unique in most cases. This section searches the Pareto-Optimal points, and analyzes the necessary and sufficient conditions for a point to be Pareto optimal.

Note that from (3), colluders in SC^b can increase their payoff if and only if they select a smaller β.

Necessary Condition: If a point is Pareto-Optimal, then decreasing μ_b and increasing the payoff of those colluders in SC^b must increase $\mu_{b,e}$ and decrease $\pi_{b,e}$. Note that from (3), μ_b is an increasing function of β. Thus, If a point is a Pareto-Optimal point, $\mu_{b,e}$ must be a decreasing function of β, which happens only when $\mu_{b,e} = \mu_{b,e}^c$. Consequently, if a point is Pareto-Optimal, β must satisfy (8), and (8) is the necessary condition of a Pareto Optimal point.

Sufficient Condition: If $\mu_{b,e} = \mu_{b,e}^c$, then to increase the payoff of those colluders in $SC^{b,e}$, colluders must decrease $\mu_{b,e}$ by selecting a larger β. However, a larger β implies a larger μ_b, thus, it decreases the payoff of those colluders in SC^b. Consequently, those points that satisfy (8) are Pareto-Optimal points, and (8) is the sufficient condition of Pareto-Optimal.

To collude, the collusion is Pareto-Optimal if and only if $\mu_{b,e} = \mu_{b,e}^c$ and (8) is satisfied, which is the curve segment in Figure 1.

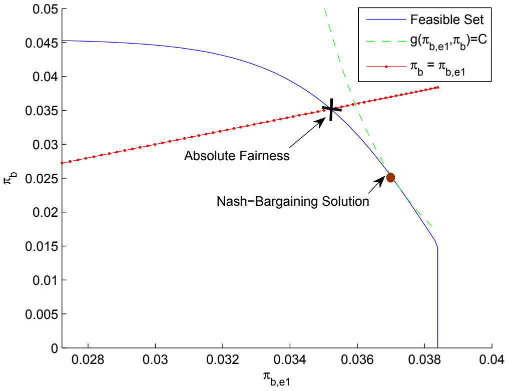

Fig. 1. Feasible set of the collusion game using the payoff function $\pi^{(i)} = (1-P_d^{(i)})^4 F/K$, with $P_{fa} = 10^{-3}$, $N_b = N_e = 50000$, $K^b = 55$, $K^{b,e} = 165$, and $K = K^b + K^{b,e}$. $|U^b| = |U^{b,e}| = 250$.

3.3. Nash-Bargaining Solution

There are many ways for colluders to share the risk and the profit, depending on their definition of "fairness". Absolute fairness is widely adopted in the literature, where all colluders have the same payoff. Colluders may also select proportional fairness, where some colluders benefit more at a cost of higher risk. One popular solution is the Nash-Bargaining solution, which is based on the idea that players who can gain more will naturally ask for more in the bargain. The Nash-Bargaining solution is based on the definition of fairness that the additional payoff must be divided between the two players in a ratio equal to the rate at which this utility can be transferred.

Mathematically speaking, the Nash-Bargaining solution maximizes the product of the utility gain. In our problem, the Nash-Bargaining solution $(\overline{\pi}_{b,e}, \overline{\pi}_b)$ maximizes

$$g(\pi_{b,e}, \pi_b) = (\pi_{b,e} - \pi_{b,e}^*)^{K^{b,e}} (\pi_b - \pi_b^*)^{K^b}$$
$$\text{where } \pi_{b,e}^* = \min_\beta \pi_{b,e}, \pi_b^* = \min_\beta \pi_b. \quad (9)$$

The Nash-Bargaining solution is in the Pareto-Optimal set and, therefore, it always satisfies (7). Consequently, (9) becomes:

$$g(\beta) = A(\beta)^{K^{b,e}} B(\beta)^{K^b}, \text{ where}$$
$$B(\beta) = \left[1 - Q\left(\frac{h - \frac{\beta\sqrt{N_b}}{K^b}\sigma_w}{\sigma_n}\right)\right]^{\gamma_1} - \left[1 - Q\left(\frac{h - \frac{\sqrt{N_b}}{K^b}\sigma_w}{\sigma_n}\right)\right]^{\gamma_1}$$
$$A(\beta) = \left[1 - Q\left(\frac{h - \frac{(1-\beta)N_b+N_e}{K^b\sqrt{N_b+N_e}}\sigma_w}{\sigma_n}\right)\right]^{\gamma_1}$$
$$- \left[1 - Q\left(\frac{h - \frac{\sqrt{N_b+N_e}}{K^{b,e}}\sigma_w}{\sigma_n}\right)\right]^{\gamma_1} \quad (10)$$

Note that Nash-Bargaining solution is always Pareto-Optimal and the set of β corresponding to the Pareto-Optimal points is closed. Thus, $g(\beta)$ is a concave function, annd it is maximized when the gradient of $g(\beta)$ equals to zero or when β is on the boundary.

From (10), if $g'(\beta) = 0$, then

$$K^{b,e} A'(\beta) B(\beta) = K^b A(\beta) B'(\beta) \quad (11)$$

Where $A'(\beta)$ and $B'(\beta)$ are the derivatives of $A(\beta)$ and $B(\beta)$ over β. Note that both $B(\beta)$ and $A'(\beta)$ are increasing functions of β,

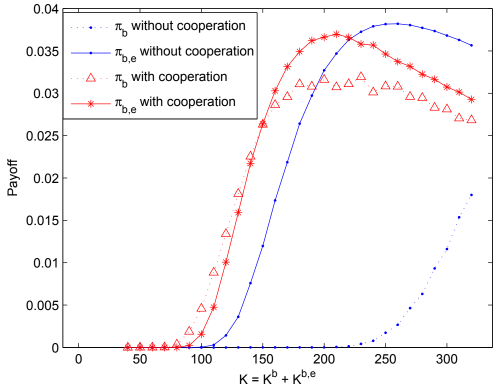

Fig. 2. Colluders' payoffs π_b and $\pi_{b,e}$. $P_{fa} = 10^{-3}$, $N_b = N_e = 50000$, $K^b : K^{b,e} = 1 : 3$, and $|U^b| = |U^{b,e}| = 250$.

while $A(\beta)$ and $B'(\beta)$ are decreasing functions of β. Thus, the solution of (11) is a monotonically decreasing function of $K^b/K^{b,e}$. It implies that the subgroup of colluders with a larger size benefits more than the others.

4. SIMULATION RESULTS

In our simulations, we first generate independent vectors following Gaussian distribution $\mathcal{N}(0, 1)$, and then apply Gram-Schmidt orthogonalization to generate orthogonal fingerprints. The lengths of the fingerprints embedded in the base layer and the enhancement layer are $N_b = N_e = 50000$, and both two layers contain 20 frames, respectively. The total number of users is 500, where $U^b = U^{b,e}$. The probability of accusing an innocent user, P_{fa}, is 10^{-3}. $K^b/K = 1/4$ of them receive the fingerprinted base layer only, and the other $K^{b,e}/K = 3/4$ of the colluders receive fingerprinted copies of high resolution.

Figure 1 shows the corresponding feasible set when there are totally 220 colluders. Define $\mathcal{C}$ as the set of all the cs where the intersections of the curve $g(\pi_{b,e}, \pi_b) = c$ and the feasible set are not empty. Mathematically speaking, the Nash-Bargaining solution is the intersection of the Pareto-optimal set and the curve $g(\pi_{b,e}, \pi_b) = \max\{\mathcal{C}\}$. Since the boundary of the Pareto-optimal set is a strictly concave function and $g(\pi_{b,e}, \pi_b) = c$ is strictly convex, the Nash-Bargaining solution is unique. In Figure 1, the dot is the Nash-Bargaining solution and the cross is the absolute fairness solution. It is clear that the Nash-Bargaining solution favors the group with more colluders, which is $SC^{b,e}$ in our simulation setup.

Figure 2 shows colluders' payoffs, and Figure 3 plots their probability of being detected. In our simulations, we consider two scenarios: attackers only collude with those from their own subgroup (i.e., an attacker who receives a high-resolution copy will only collude with those in $SC^{b,e}$ but not those in SC^b.); and attackers also collude with those from the other subgroup. From Figure 3, colluding with more attackers further reduces colluder i's risk of being detected. However, from Figure 2, it does not necessarily always increase his/her payoff since he/she has to share the profit with more people. For example, when $K^{b,e} = 240$ and $K^b = 80$, for those colluders in $SC^{b,e}$, colluding with SC^b reduces their risk from 0.03 to 0.02; while it also lowers their payoff because they have to share the profit with 80 more people. Therefore, in this scenario, colluders in $SC^{b,e}$ may prefer not to collude with those in SC^b.

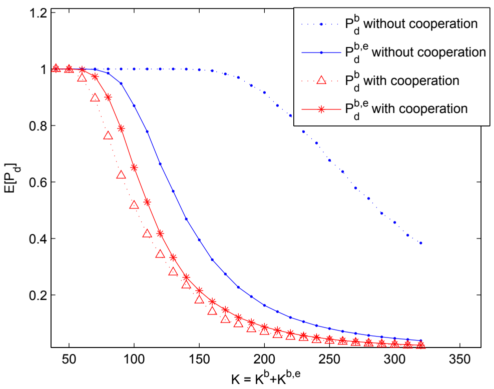

Fig. 3. Colluders' average probability of being detected $E[P_d^{(i)}]$ for $i \in SC^b$ and $i \in SC^{b,e}$. $P_{fa} = 10^{-3}$, $N_b = N_e = 50000$, $K^b : K^{b,e} = 1 : 3$, and $|U^b| = |U^{b,e}| = 250$.

5. CONCLUSIONS

This paper studies the game-theoretic modelling and analysis of the dynamics among colluders to achieve fairness of collusion. We model the fairness dynamics among colluders as a non-cooperative game, where each colluder aims to maximize his/her own payoff function under the fairness constraint. We analyze the feasible set of the game; study the Pareto-Optimal set where no colluder can further increase his/her payoff without decreasing others'; and find the Nash-Bargaining solution of the game. Our analysis shows that during collusion, colluders choose different points in the feasible set, depending on the colluders' definition of "fairness" and their agreement on how to distribute the risk and the profit among themselves.

6. REFERENCES

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

[2] J. Su, J. Eggers, and B. Girod, "Capacity of digital watermarks subject to an optimal collusion attacks," *European Signal Processing Conference (EUSIPCO 2000)*, 2000.

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

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

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

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

[7] 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. on Image Processing*, vol. 14, no. 6, pp. 804–821, June 2005.

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