Risk-Distortion Analysis for Video Collusion Attacks: A Mouse-and-Cat Game

Yan Chen, *Student Member, IEEE*, W. Sabrina Lin, *Member, IEEE*, and K. J. Ray Liu, *Fellow, IEEE*

***Abstract*—Copyright protection is a key issue for video sharing over public networks. To protect the video content from unauthorized redistribution, digital fingerprinting is commonly used. To develop an efficient collusion-resistant fingerprinting scheme, it is very important for the system designer to understand how the behavior dynamics of colluders affect the performance of collusion attack. In the literature, little effort has been made to explicitly study the relationship between risk, e.g., the probability of the colluders to be detected, and the distortion of the colluded signal. In this paper, we investigate the risk-distortion relationship for the linear video collusion attack with Gaussian fingerprint. We formulate the optimal linear collusion attack as an optimization problem of finding the optimal collusion parameters to minimize the distortion subject to a risk constraint. By varying the risk constraint and solving the corresponding optimization problem, we can derive the optimal risk-distortion curve. Moreover, based upon the observation that the detector/attacker can each improve the detection/attack performance with the knowledge of his/her opponent's strategy, we formulate the attack and detection problem as a dynamic *mouse and cat* game and study the optimal strategies for both the attacker and detector. We show that if the detector uses a fixed detection strategy, the attacker can estimate the detector's strategy and choose the corresponding optimal strategy to attack the fingerprinted video with a small distortion. However, if the detector is powerful, i.e., the detector can always estimate the attacker's strategy, the best strategy for the attacker is the min-max strategy. Finally, we conduct several experiments to verify the proposed risk-distortion model using real video data.**

***Index Terms*—Game theory, fingerprint, risk distortion, video collusion.**

I. Introduction

With the explosive growth of the Internet and the advance of the compression technologies, video sharing over public networks becomes more and more popular. This phenomenon causes a critical problem to digital content providers since their materials can be easily duplicated and distributed without authorization. Digital fingerprinting is one of the most important techniques for tracing the distribution of video contents and protecting them from illegal usage [1]. It embeds a unique identification information, which serves as a digital fingerprint, into each distributed copy of video. When a copy is redistributed without authorization, the content providers can extract the embedded fingerprint to trace back the source of the leak.

To reduce the probability of being detected, attackers may apply various attacks to remove the fingerprints before redistribution. One common and effective attack against digital fingerprinting is collusion attack [2]–[4], where a group of attackers combine information from their copies to generate a new colluded copy in which the original fingerprints are removed or attenuated. In [5], several types of collusion attacks, including a few nonlinear collusion attacks, have been studied. The simulation results in [5] show that nonlinear attacks are more effective than average attack for uniformly distributed fingerprints, and normally distributed fingerprints are more robust against nonlinear collusion attacks than uniformly distributed fingerprints. Later in [6], the analytical study on the performance of Gaussian fingerprints was provided. The study shows that for Gaussian fingerprints with spread spectrum embedding, a number of nonlinear collusion attacks based upon order statistics, such as minimum and min-max attacks, can be well approximated by averaging collusion plus additive white Gaussian noise. Similar conclusions can be also found in [7]–[9].

Most of the existing studies of collusion attack focus on image collusion attack, where the host (source) signals are the same. In this case, if no postprocessing techniques such as blurring and sharpening are performed, the difference between the colluded copy and the original copy is usually smaller than the difference between the distributed copy and the original copy since the fingerprint is removed or attenuated during the collusion process. However, this conclusion is not true if the host signals are video sequences [10]. Video data have a unique characteristic that the temporally adjacent frames are similar but usually not identical. Therefore, for video collusion attacks, not only the intercopy attack which combines the frames among different copies, but also the intracopy attack which combines temporally adjacent frames within the same copy, can be conducted.

Due to the dissimilarity of the temporally adjacent frames, distortion would be introduced during intracopy attack. Therefore, for video collusion attack, there exists a tradeoff between the fingerprint remained in the colluded copy, which corresponds to the probability of being detected, i.e., the risk for the colluders, and the quality of the colluded copy, i.e., the distortion. It is extremely important for the colluders to learn the risk-distortion tradeoff since knowing this tradeoff would help them choose the best strategy when generating colluded copy. It is also essential for the detectors to understand the risk-distortion tradeoff since it would help them predict the

Manuscript received June 05, 2009; revised February 08, 2010. First published March 11, 2010; current version published June 16, 2010. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Arun Abraham Ross.

The authors are with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA (e-mail: yan@umd.edu; wylin@umd.edu; 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/TIP.2010.2045030

behavior of the colluders and, hence, help them design an anti-collusion strategy.

In [10], the authors investigate some possible strategies of selfish colluders and show that a selfish colluder can deviate from agreement to further reduce his/her risk by choosing the optimal temporal filtering. Nevertheless, the optimal risk-distortion tradeoff has not been fully studied yet. Motivated by [10], in this paper, we explicitly explore the relationship between risk and distortion by conducting a theoretical analysis for the linear video collusion attack with Gaussian fingerprinting. We formulate the risk and distortion as functions of the temporal filter coefficients, and model the collusion attack as an optimization problem of finding the optimal coefficients to minimize the distortion subject to a given risk constraint. By varying the risk constraint and solving the corresponding optimization problem, we can derive the optimal risk-distortion curve.

Moreover, we show that the detector can improve his/her detection performance given the optimal coefficients the attacker uses, and similarly the attacker can improve his/her attack performance given the optimal coefficients the detector uses. According to this observation, we formulate the attack and detection problem as a dynamic ***mouse and cat*** game and study the optimal strategy for the attacker/detector given the knowledge of his/her opponent's strategy. In practice, since the attacker needs to choose his/her strategy first, a powerful detector will always be able to estimate the attacker's strategy. In such a case, we show that the best strategy for the attacker is the min-max strategy, i.e., to minimize the risk by assuming the detector has the perfect knowledge of the attacker's strategy. We also discuss the min-max strategy of the attackers when the attackers consider the additive white Gaussian noise (AWGN) to further reduce their risk. Finally, we conduct several experiments to verify the proposed risk-distortion model using real video data.

The rest of this paper is organized as follows. Section II describes the system models. In Section III, we conduct a theoretical analysis for the linear collusion attack and derive the risk-distortion relationship. Section IV discusses the optimal strategy for the attacker and detector when knowing his/her opponent's strategy. In Section V, we discuss the min-max strategy for the attacker in the worst-case scenario. The parameter estimation and experimental results are shown in Sections VI and VII. Finally, the conclusion is drawn in Section VIII.

II. System Models

In this section, we will introduce the system model, including video fingerprint embedding, detection, and collusion attack model.

A. Fingerprint Embedding

Let $I(t)$ be the t^{th} frame of the host video sequence, which can be the pixel values or the DCT coefficients. Let $f_k(t)$ and $W_k(t)$ be the t^{th} frame of fingerprinted video and fingerprint signal for user k, respectively. Then, the fingerprint embedding process of the t^{th} frame for the k^{th} user can be written as

$$f_k(t) = I(t) + W_k(t). \tag{1}$$

Note that the fingerprint signal should be scaled according to some parameters to achieve the imperceptibility. In such a case, we can define $W_k(t) = \alpha(t) \cdot \times w_k(t)$, where $w_k(t)$ is the original fingerprint signal, $\alpha(t)$ is the parameter used to control the energy of the embedded fingerprint to achieve the imperceptibility, and $\cdot\times$ represents the Hadamard product.

To simplify the analysis, the orthogonal fingerprint modulation is used [10], [11], i.e., $E[W_i(t)^T W_j(t)] = \sigma_w^2 \delta_{i,j}$, where $\delta_{i,j} = 1$ if $i = j$ and $\delta_{i,j} = 0$ if $i \neq j$. Moreover, to resist intracopy collusion attack [12], [13], the fingerprint W_k between neighboring frames for the same user k are correlated with each other, while the correlation is determined by the similarity of the host frames and the temporal distance of the indices [12] as given by

$$\rho[W_k(t_1), W_k(t_2)] = \gamma^{|t_1 - t_2|} \rho[I(t_1), I(t_2)] \tag{2}$$

where $\rho[A, B] = cov(A, B)/\sqrt{var(A)var(B)}$ is the statistical correlation coefficient between random variables A and B, and γ is a scaling parameter $(0 \leq \gamma \leq 1)$ that controls the tradeoff between the visual quality and the degree of the resistance. If γ is large, then the degree of the resistance against the intracopy attack is high. However, the visual quality of the fingerprinted video becomes poor due to the veiling artifacts. On the contrary, if γ is small, then the veiling artifacts are less significant, while the fingerprinted video becomes vulnerable to the intracopy attack.

B. Fingerprint Detection

Once the content owners find a suspicious copy, he/she can use correlation-based fingerprint detection to identify the attackers [1]. Without loss of generality, we analyze the frame-based detection. Similar analysis can be easily extended to Group-Of-Picture (GOP) based or sequence-based detection [6]. For each frame $\hat{f}(t)$, the detector extracts the fingerprint using

$$\hat{W}(t) = \hat{f}(t) - I(t). \tag{3}$$

Then, for each user k who receives frame t, compute the detection statistics using

$$TN_k(t) = \frac{W_k^T(t)\hat{W}(t)}{\sqrt{W_k^T(t)W_k(t)}}. \tag{4}$$

Finally, given a threshold h that is determined by false alarm probability (see Section III.), the estimated attacker set for frame t is $\hat{SC}(t) = \{i : TN_i(t) > h\}$. Note that the detectors can use any "postprocessing" method such as majority rule to combine the results of the frame-based detection. However, this is not the goal of this paper. In this paper, to focus on the risk-distortion relationship, we only consider the frame-based detection.

C. Video Collusion Attack Model

Without loss of generality, we focus on the case of linear collusion attacks in this paper [11]. Let M be the total number of the attackers. As shown in Fig. 1, each attacker first performs intracopy attack by applying temporal filtering on the temporally adjacent video frames. Then, all attackers would collude

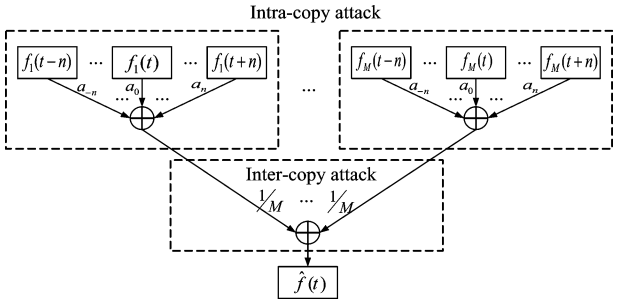

Fig. 1. Collusion attack model.

together to perform intercopy attack. Since the fingerprint in every frame for each attacker $W_k(t)$ is independent and identically distributed (i.i.d), if we assume that all attackers share the same risk, then the weights allocated to the intracopy and intercopy attacks would be the same for all attackers. Therefore, the attack model can be formulated as that a colluded frame is given by

$$\hat{f}(t) = \sum_{k=1}^{M} \frac{1}{M} \left[\sum_{i=-n}^{n} a_i f_k(t+i) \right] \tag{5}$$

where $\sum_{i=-n}^{n} a_i = 1$. The attackers are to choose a_i's to minimize the collusion distortion under a certain risk constraint, while the detector is to estimate the a_i's that attackers choose and use them as side information to improve the detection performance.

III. Risk-Distortion Analysis Framework

A. Risk of the Colluders

Given the colluded frame $\hat{f}(t)$, the detector extracts the fingerprint $\hat{W}(t)$ by

$$\hat{W}(t) = \hat{f}(t) - I(t) = \left(\mathbf{e}_I + \frac{1}{M} \sum_{i=1}^{M} \mathbf{W}_i \right) \mathbf{a} \tag{6}$$

where $\mathbf{e}_I = [I(t-n) - I(t), \ldots, I(t+n) - I(t)]$, $\mathbf{W}_i = [W_i(t-n), \ldots, W_i(t+n)]$, and $\mathbf{a} = [a_{-n}, \ldots, a_n]^T$.

According to (4), the detection statistics $TN_k(t)$ can be written as

$$\begin{aligned} TN_k(t) &= \frac{W_k^T(t)\hat{W}(t)}{\sqrt{W_k^T(t)W_k(t)}} \\ &= \frac{W_k^T(t)\left[\mathbf{e}_I\mathbf{a} + \frac{1}{M}\sum_{i=1}^{M}\mathbf{W}_i\mathbf{a}\right]}{\sqrt{W_k^T(t)W_k(t)}}. \end{aligned} \tag{7}$$

In this paper, we assume that the residues are independent and identically distributed (i.i.d.) Laplace variables [14], [15], i.e., $[I(t+i) - I(t)]_j \sim Laplace(0, \lambda_i)$, where $[I(t+i) - I(t)]_j$ stands for the j^{th} pixel in $[I(t+i) - I(t)]$. Note that in each frame of a video sequence with QCIF format, there are 174×144 such i.i.d. Laplace variables. Therefore, we can apply the central limit theorem to approximate the weighted sum of these 174×144 i.i.d. Laplace variables as a Gaussian random variable, i.e., $W_k^T(t)[I(t+i) - I(t)]/\sqrt{W_k^T(t)W_k(t)} \sim N(0, \sigma_i^2)$ with $\sigma_i^2 = 2\lambda_i^2$. Moreover, since the linear combination of the Gaussian distribution is also a Gaussian distribution, we have $W_k^T(t)\mathbf{e}_I\mathbf{a}/\sqrt{W_k^T(t)W_k(t)} \sim N(0, \|\Lambda\mathbf{a}\|_2^2)$, where $\Lambda = diag\{\sigma_{-n}, \ldots, \sigma_n\}$ and $\|\Lambda\mathbf{a}\|_2$ is $L2$-norm of $\Lambda\mathbf{a}$. Then, we know from (7) that the detection statistics of attacker k, $TN_k(t)$, satisfies Gaussian distribution $N(\mu_k, \|\Lambda\mathbf{a}\|_2^2)$ [16], where the mean μ_k is given by

$$\mu_k = E\left[\frac{\hat{W}^T(t)W_k(t)}{\sqrt{W_k^T(t)W_k(t)}} \right] = \frac{1}{M}\mathbf{p}^T\mathbf{a} \tag{8}$$

with

$$\mathbf{p} = \left[E\left[\frac{W_k^T(t-n)W_k(t)}{\sqrt{W_k^T(t)W_k(t)}} \right], \ldots, E\left[\frac{W_k^T(t+n)W_k(t)}{\sqrt{W_k^T(t)W_k(t)}} \right] \right]^T. \tag{9}$$

Let R, the risk of the colluder, be the probability of being detected. Given a detection threshold h, according to (7) and (8), the risk R can be computed by

$$R = \text{Prob}(TN_k(t) > h) = Q\left(\frac{h - \frac{1}{M}\mathbf{p}^T\mathbf{a}}{\|\Lambda\mathbf{a}\|_2} \right) \tag{10}$$

where $Q(x)$ is the Gaussian tail function

$$\int_x^\infty 1/\sqrt{2\pi}\exp^{-x^2/2}\,dx.$$

Similarly, the detection statistics of an innocent user satisfies Gaussian distribution $N(0, \|\Lambda\mathbf{a}\|_2^2)$ [16]. Therefore, the probability of an innocent user to be falsely detected as an attacker, i.e., P_{fa}, is given by

$$P_{fa} = Q\left(\frac{h}{\|\Lambda\mathbf{a}\|_2} \right). \tag{11}$$

From (10) and (11), we can see that the threshold h controls the tradeoff between the positive detection probability R and the false alarm probability P_{fa}. If the desired false alarm probability P_{fa} is α, then $h = Q^{-1}(\alpha)\|\Lambda\mathbf{a}\|_2$ and the risk R becomes

$$R = Q\left(\frac{Q^{-1}(\alpha)\|\Lambda\mathbf{a}\|_2 - \frac{1}{M}\mathbf{p}^T\mathbf{a}}{\|\Lambda\mathbf{a}\|_2} \right). \tag{12}$$

B. Distortion of the Colluded Frame

From (6), we can see that the difference between the attacked frame $\hat{f}(t)$ and the original frame $I(t)$ is $\hat{W}(t)$. Therefore, the distortion D of the colluded copy, which is defined as the mean square of the difference, can be computed by

$$D = E\left[\hat{W}^T(t)\hat{W}(t) \right] = \mathbf{a}^T\mathbf{K}\mathbf{a} \tag{13}$$

where $\mathbf{K} = E[\mathbf{e}_I^T\mathbf{e}_I] + 1/ME[\mathbf{W}_1^T\mathbf{W}_1]$ and the second equality follows from the independence between I and W_k and $E[\mathbf{W}_1^T\mathbf{W}_1] = E[\mathbf{W}_k^T\mathbf{W}_k]$, for all k.

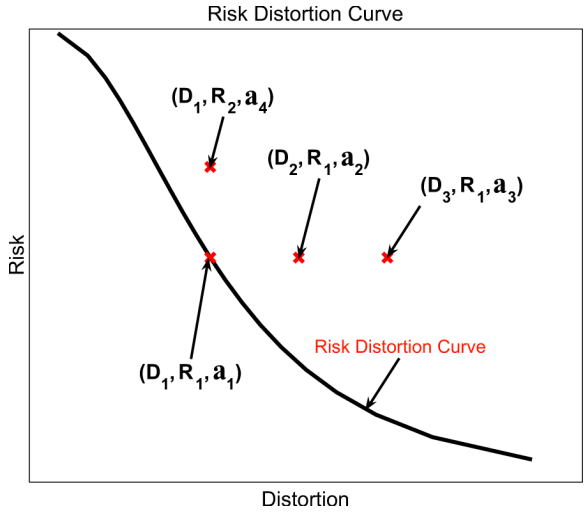

Fig. 2. Risk distortion curve.

C. Risk-Distortion Relationship

From (12) and (13), we can see that both the distortion and risk are determined by the coefficients of the temporal filter $\mathbf{a}$. In Fig. 2, we show the risk distortion plot using different coefficients. We can see that, for a fixed risk R_1, there are several different coefficients, $\mathbf{a}_1$, $\mathbf{a}_2$, and $\mathbf{a}_3$, which would lead to different amounts of distortions, D_1, D_2, and D_3. A rational attacker will choose the optimal coefficient $\mathbf{a}$ that minimizes the distortion to generate the colluded copy, which leads to the risk distortion curve. Therefore, the attacker's problem can be formulated as

$$\begin{aligned} \min_{\mathbf{a}} \quad & \frac{1}{2}D = \frac{1}{2}\mathbf{a}^T\mathbf{K}\mathbf{a} \\ s.t. \quad & R = Q\left(\frac{Q^{-1}(\alpha)\|\Lambda\mathbf{a}\|_2 - \frac{1}{M}\mathbf{p}^T\mathbf{a}}{\|\Lambda\mathbf{a}\|_2}\right) \le R_0 \\ & \mathbf{1}^T\mathbf{a} = 1 \end{aligned} \tag{14}$$

where the scale factor $1/2$ in the objective function is only for computation convenience.

Obviously, the previously shown optimization problem is nonconvex since the quadratic term $\|\Lambda\mathbf{a}\|_2$ is in the denominator, which makes the first constraint nonconvex. However, since the Gaussian tail function $Q(x)$ is a monotonically decreasing function, we can rewrite the optimization problem as

$$\begin{aligned} \min_{\mathbf{a}} \quad & \frac{1}{2}D = \frac{1}{2}\mathbf{a}^T\mathbf{K}\mathbf{a} \\ s.t. \quad & \left[Q^{-1}(R_0) - Q^{-1}(\alpha)\right]\|\Lambda\mathbf{a}\|_2 + \frac{1}{M}\mathbf{p}^T\mathbf{a} \le 0 \\ & \mathbf{1}^T\mathbf{a} = 1. \end{aligned} \tag{15}$$

The optimization problem shown previously is a quadratically constrained quadratic program (QCQP) problem [17]. If $Q^{-1}(R_0) \ge Q^{-1}(\alpha)$, i.e., $R_0 \le \alpha$, the problem is a convex optimization problem. We can find the optimal solution using numerical methods, e.g., the interior point methods [17].

If $Q^{-1}(R_0) < Q^{-1}(\alpha)$, which means $R_0 > \alpha$, the problem is nonconvex. In general, a nonconvex QCQP problem is a NP-hard problem [17] and it is very difficult to find the global optimal solution. However, by approximating the concave term with its first-order Taylor expansion, a locally optimal solution can be solved using constrained concave-convex crocedure (CCCP) [18]. And the relaxed optimization problem becomes

$$\begin{aligned} \min_{\mathbf{a}} \quad & \frac{1}{2}D = \frac{1}{2}\mathbf{a}^T\mathbf{K}\mathbf{a} \\ s.t. \quad & \left[Q^{-1}(R_0) - Q^{-1}(\alpha)\right]\frac{\mathbf{a}^{(t)^T}\Lambda^T\Lambda\mathbf{a}}{\|\Lambda\mathbf{a}^{(t)}\|_2} + \frac{1}{M}\mathbf{p}^T\mathbf{a} \le 0 \\ & \mathbf{1}^T\mathbf{a} = 1. \end{aligned} \tag{16}$$

Given an initial $\mathbf{a}^{(0)}$, CCCP computes $\mathbf{a}^{(t+1)}$ from $\mathbf{a}^{(t)}$ iteratively using (16). It can be shown that CCCP converges to a locally optimal solution of the original optimization problem (14) [19].

According to (15) and (16), the optimal coefficients $\mathbf{a}$ that minimizes the distortion subject to a predefined risk constraint R_0 can be found using numerical optimization methods. Then, the minimal distortion given risk R_0 can be computed using (12). In this way, the optimal risk-distortion relationship for the colluders can be obtained. Now the only question is how to find a good initial $\mathbf{a}^{(0)}$ for the CCCP process to converge to a good local optimum.

D. Initialization for CCCP

According to (15), the reason that we need to use CCCP to find the locally optimal solution is the quadratic term $\|\Lambda\mathbf{a}\|_2$ in the constraint. In the case that $\|\Lambda\mathbf{a}\|_2$ is around a constant β, we can relax the optimization problem by approximating $\|\Lambda\mathbf{a}\|_2$ with β. Then, the relaxed optimization problem becomes

$$\begin{aligned} \min_{\mathbf{a}} \quad & \frac{1}{2}D = \frac{1}{2}\mathbf{a}^T\mathbf{K}\mathbf{a} \\ s.t. \quad & \frac{1}{M}\mathbf{p}^T\mathbf{a} - \eta \le 0 \\ & \mathbf{1}^T\mathbf{a} = 1 \end{aligned} \tag{17}$$

where $\eta = [Q^{-1}(\alpha) - Q^{-1}(R_0)]\beta$.

From (17), we can see that the objective function is quadratic and the constraints are linear. The optimization problem is a quadratic problem, which is convex. The optimal solution for the relaxed problem can be found by solving the KKT conditions [17] and

$$\mathbf{a}^{(0)} = \mathbf{K}^{-1}\begin{bmatrix}\frac{1}{M}\mathbf{p} & \mathbf{1}\end{bmatrix}\begin{bmatrix}\frac{1}{M^2}\mathbf{p}^T\mathbf{K}^{-1}\mathbf{p} & \frac{1}{M}\mathbf{p}^T\mathbf{K}^{-1}\mathbf{1} \\ \frac{1}{M}\mathbf{1}^T\mathbf{K}^{-1}\mathbf{p} & \mathbf{1}^T\mathbf{K}^{-1}\mathbf{1}\end{bmatrix}^{-1}\begin{bmatrix}\eta \\ 1\end{bmatrix}. \tag{18}$$

Remark:

- From (18), we can see that $\mathbf{a}^{(0)}$ is determined by $\eta = [Q^{-1}(\alpha) - Q^{-1}(R_0)]\beta$, which means that the initialization of $\mathbf{a}^{(0)}$ reduces to finding a good value for β.
- Since (18) is derived based upon the assumption that $\|\Lambda\mathbf{a}\|_2$ is around a constant β, $\mathbf{a}^{(0)}$ is a good initial point if β is around $\|\Lambda\mathbf{a}^\star\|_2$, where $\mathbf{a}^\star$ is the optimal $\mathbf{a}$.

IV. Optimal Strategies for the Detector and Attacker

From the previous section, we can see that attackers can obtain the risk distortion curve based upon the assumption that the

detector uses the fingerprint of the current frame to compute the detection statistics. However, if knowing that attackers use a linear filter to attack the fingerprint, the detector will modify the detection statistics to improve the detection performance. On the other hand, if attackers know that the detector changes his/her detection statistics, they will change their strategy accordingly. Therefore, there exists a dynamic between attackers and detector and the problem can be formulated as a ***mouse and cat*** game, where the optimal strategy for the attacker (detector) lies on his/her opponent's strategy. Since the risk distortion curve is determined by the optimal coefficient $\mathbf{a}^\star$, we regard the optimal coefficient $\mathbf{a}^\star$ as side information to be estimated or guessed by both parties. In this section, we will discuss how the detector and attackers choose their optimal strategies based upon the side information.

A. Optimal Strategy for the Detector With Side Information

If the detector knows (estimates) that the attacker uses the linear filter with optimal coefficients $\mathbf{a}_a^\star$ to attack the fingerprint, the detector will modify the detection statistics to improve the detection performance. Suppose that the detector use linear combination of the fingerprint, i.e., $\mathbf{W}_k\mathbf{a}$, to compute the detection statistics, then the detection statistics become

$$TN_k'(t) = \frac{\mathbf{a}^T\mathbf{W}_k^T\left(\mathbf{e}_I + \frac{1}{M}\sum_{i=1}^{M}\mathbf{W}_i\right)\mathbf{a}_a^\star}{\|\mathbf{W}_k\mathbf{a}\|_2}. \tag{19}$$

From (19), we know that $TN_k'(t)$ satisfies Gaussian distribution $N\left(1/ME\left[\mathbf{a}^T\mathbf{W}_k^T\mathbf{W}_k\mathbf{a}_a^\star/\|\mathbf{W}_k\mathbf{a}\|_2\right], \|\Lambda\mathbf{a}_a^\star\|_2\right)$. Therefore, given the false alarm probability $P_{fa} = \alpha$, the risk of the attacker is

$$R = Q\left(\frac{Q^{-1}(\alpha)\|\Lambda\mathbf{a}_a^\star\|_2 - \frac{1}{M}E\left[\frac{\mathbf{a}^T\mathbf{W}_k^T\mathbf{W}_k\mathbf{a}_a^\star}{\|\mathbf{W}_k\mathbf{a}\|_2}\right]}{\|\Lambda\mathbf{a}_a^\star\|_2}\right). \tag{20}$$

Obviously, a rational detector will choose the optimal coefficient $\mathbf{a}$ to maximize the probability of catching the attackers, which is the risk of the attackers. According to (20), maximizing R is equivalent to maximizing $E\left[\mathbf{a}^T\mathbf{W}_k^T\mathbf{W}_k\mathbf{a}_a^\star/\|\mathbf{W}_k\mathbf{a}\|_2\right]$, which results in new optimal coefficient $\mathbf{a}_d^\star$ as

$$\mathbf{a}_d^\star = \mathbf{a}_a^\star. \tag{21}$$

Therefore, if the detector knows that the attacker uses the linear filter with optimal coefficients $\mathbf{a}_a^\star$ to attack the fingerprint, he/she will also use $\mathbf{W}_k\mathbf{a}_a^\star$ to compute the detection statistics since it can give the best detection performance.

B. Optimal Strategy for the Attackers With Side Information

On the other hand, if knowing that the detector will use the linear filter with coefficient $\mathbf{a}_d^\star$ to compute the detection statistics, obviously the attackers will try to reduce their risk by using another linear filter to attack the fingerprint. Let $\mathbf{a}$ be the new coefficients the attackers use, then the detection statistics become

$$TN_k''(t) = \frac{\mathbf{a}_d^{\star T}\mathbf{W}_k^T\left(\mathbf{e}_I + \frac{1}{M}\sum_{i=1}^{M}\mathbf{W}_i\right)\mathbf{a}}{\|\mathbf{W}_k\mathbf{a}_d^\star\|_2}. \tag{22}$$

Similar to $TN_k'(t)$, $TN_k''(t)$ satisfies Gaussian distribution $N\left(1/ME\left[\mathbf{a}_d^{\star T}\mathbf{W}_k^T\mathbf{W}_k\mathbf{a}/\|\mathbf{W}_k\mathbf{a}_d^\star\|_2\right], \|\Lambda\mathbf{a}\|_2\right)$. Therefore, given the false alarm probability $P_{fa} = \alpha$, the risk of the attacker to be detected becomes

$$R = Q\left(\frac{Q^{-1}(\alpha)\|\Lambda\mathbf{a}\|_2 - \frac{1}{M}E\left[\frac{\mathbf{a}_d^{\star T}\mathbf{W}_k^T\mathbf{W}_k\mathbf{a}}{\|\mathbf{W}_k\mathbf{a}_d^\star\|_2}\right]}{\|\Lambda\mathbf{a}\|_2}\right). \tag{23}$$

Surely, a rational attacker will choose the optimal coefficient $\mathbf{a}$ to minimize the risk defined in (23). And the problem can be formulated as

$$\begin{aligned}\min_{\mathbf{a}} \quad & R = Q\left(\frac{Q^{-1}(\alpha)\|\Lambda\mathbf{a}\|_2 - \frac{1}{M}E\left[\frac{\mathbf{a}_d^{\star T}\mathbf{W}_k^T\mathbf{W}_k\mathbf{a}}{\|\mathbf{W}_k\mathbf{a}_d^\star\|_2}\right]}{\|\Lambda\mathbf{a}\|_2}\right)\\ s.t. \quad & D = \mathbf{a}^T\mathbf{K}\mathbf{a} \le D_0\\ & \mathbf{1}^T\mathbf{a} = 1\end{aligned} \tag{24}$$

where D_0 is the distortion when $\mathbf{a}_d^\star$ is used for collusion.

Since the Gaussian tail function $Q(x)$ is a monotonically decreasing function, we can rewrite the optimization problem as

$$\begin{aligned}\min_{\mathbf{a}} \quad & \frac{\frac{\mathbf{a}_d^{\star T}\mathbf{W}_k^T\mathbf{W}_k\mathbf{a}}{\|\mathbf{W}_k\mathbf{a}_d^\star\|_2}}{\|\Lambda\mathbf{a}\|_2}\\ s.t. \quad & D = \mathbf{a}^T\mathbf{K}\mathbf{a} \le D_0\\ & \mathbf{1}^T\mathbf{a} = 1\end{aligned} \tag{25}$$

which is equivalent to

$$\begin{aligned}\min_{\mathbf{a},\xi} \quad & \xi\\ s.t. \quad & \frac{\mathbf{a}_d^{\star T}\mathbf{W}_k^T\mathbf{W}_k\mathbf{a}}{\|\mathbf{W}_k\mathbf{a}_d^\star\|_2} - \xi\|\Lambda\mathbf{a}\|_2 \le 0\\ & D = \mathbf{a}^T\mathbf{K}\mathbf{a} \le D_0\\ & \mathbf{1}^T\mathbf{a} = 1.\end{aligned} \tag{26}$$

Thus, we can find the solution iteratively by solving the following optimization problem:

$$\begin{aligned}\min_{\mathbf{a}^{(t)}} \quad & \frac{\mathbf{a}_d^{\star T}\mathbf{W}_k^T\mathbf{W}_k\mathbf{a}^{(t)}}{\|\mathbf{W}_k\mathbf{a}_d^\star\|_2} - \xi^{(t)}\|\Lambda\mathbf{a}^{(t)}\|_2\\ s.t. \quad & D = \mathbf{a}^{(t)^T}\mathbf{K}\mathbf{a}^{(t)} \le D_0\\ & \mathbf{1}^T\mathbf{a}^{(t)} = 1\end{aligned} \tag{27}$$

with $\xi^{(t+1)} = \mathbf{a}_d^{\star T}\mathbf{W}_k^T\mathbf{W}_k\mathbf{a}^{(t)}/\|\mathbf{W}_k\mathbf{a}_d^\star\|_2/\|\Lambda\mathbf{a}^{(t)}\|_2$, and t is the iteration index. Notice that at each iteration, if $\xi^{(t)} \le 0$, the optimization problem in (27) is convex, the global optimal solution can be found using numerical method. However, if $\xi^{(t)} > 0$,

the optimization problem in (27) is nonconvex. Then, we need to use CCCP to find the locally optimal solution.

V. Min-Max Strategy for the Attacker: The Worst-Case Scenario

In the previous section, we discuss the optimal strategy of the detector and attacker with side information, i.e., how the detector and attacker should react based upon the knowledge of his/her opponent's strategy. However, in reality, the attacker needs to choose his/her strategy first. Then, the detector will choose his/her strategy to detect the attacker. In this sense, the best-case scenario for the attacker is that the detector uses a fixed strategy which is known by the attacker. In such a best-case scenario, the attacker's optimal strategy can be found by solving (27). On the other hand, the worst-case scenario for the attacker is that the detector has the full knowledge of the attacker's strategy and choose his/her optimal strategy based upon the attacker's strategy. In such a worst-case scenario, the attacker's optimal strategy is the min-max strategy, i.e., to minimize the worst-case risk.

A. Min-Max Strategy for the Attacker

If the attackers use a linear filter with coefficients $\mathbf{a}_a$ to attack the fingerprint and the detector uses $\mathbf{W}_k\mathbf{a}_d$ to compute the detection statistics, then the detection statistics become

$$TN_k'''(t) = \frac{\mathbf{a}_d{}^T\mathbf{W}_k^T\left(\mathbf{e}_I + \frac{1}{M}\sum_{i=1}^{M}\mathbf{W}_i\right)\mathbf{a}_a}{||\mathbf{W}_k\mathbf{a}_d||_2}. \tag{28}$$

Similar to (20) and (23), the risk of the attackers to be detected becomes

$$R = Q\left(\frac{Q^{-1}(\alpha)||\Lambda\mathbf{a}_a||_2 - \frac{1}{M}E\left[\frac{\mathbf{a}_d{}^T\mathbf{W}_k^T\mathbf{W}_k\mathbf{a}_a}{||\mathbf{W}_k\mathbf{a}_d||_2}\right]}{||\Lambda\mathbf{a}_a||_2}\right). \tag{29}$$

Obviously, a rational detector will always choose the optimal coefficients $\mathbf{a}_d$ to maximize the risk. In the worst-case scenario for the attackers, the detector has the full knowledge of the attacker's strategy $\mathbf{a}_a$. Therefore, when the detector use his/her optimal strategy, the risk of the attackers to be detected becomes

$$R(\mathbf{a}_d^\star) = \max_{\mathbf{a}_d} Q\left(\frac{Q^{-1}(\alpha)||\Lambda\mathbf{a}_a||_2 - \frac{1}{M}E\left[\frac{\mathbf{a}_d{}^T\mathbf{W}_k^T\mathbf{W}_k\mathbf{a}_a}{||\mathbf{W}_k\mathbf{a}_d||_2}\right]}{||\Lambda\mathbf{a}_a||_2}\right). \tag{30}$$

Knowing that the detector uses the optimal strategy based upon his/her strategy, a rational attacker will choose the optimal coefficients $\mathbf{a}_a$ to minimize the risk shown in (30). Therefore, the problem of finding the optimal $\mathbf{a}_a$ can be formulated as (31), shown at the bottom of the page. Therefore, the optimal strategy of the attacker in the worst-case scenario is the min-max strategy.

According to (21), we know that the optimal $\mathbf{a}_d$ is equal to $\mathbf{a}_a$. Let $\mathbf{a}_d = \mathbf{a}_a = \mathbf{a}$, then the optimization problem in (31) becomes

$$\begin{aligned} \min_{\mathbf{a}} \quad & Q\left(\frac{Q^{-1}(\alpha)||\Lambda\mathbf{a}||_2 - \frac{1}{M}E\left[||\mathbf{W}_k\mathbf{a}||_2\right]}{||\Lambda\mathbf{a}||_2}\right) \\ s.t. \quad & D = \mathbf{a}^T\mathbf{K}\mathbf{a} \le D_0 \\ & \mathbf{1}^T\mathbf{a} = 1 \end{aligned} \tag{32}$$

Similar to (27), we can find the solution iteratively by solving the following optimization problem

$$\begin{aligned} \min_{\mathbf{a}^{(t)}} \quad & ||\mathbf{W}_k\mathbf{a}^{(t)}||_2 - \xi^{(t)}||\Lambda\mathbf{a}^{(t)}||_2 \\ s.t. \quad & D = \mathbf{a}^{(t)^T}\mathbf{K}\mathbf{a}^{(t)} \le D_0 \\ & \mathbf{1}^T\mathbf{a}^{(t)} = 1 \end{aligned} \tag{33}$$

with $\xi^{(t+1)} = ||\mathbf{W}_k\mathbf{a}^{(t)}||_2/||\Lambda\mathbf{a}^{(t)}||_2$. Notice that since $\xi^{(t)} > 0$, the optimization problem in (33) is nonconvex. Therefore, we need to use CCCP to find the locally optimal solution.

B. Risk Reduction Using Additive White Gaussian Noise (AWGN)

In the previous subsection, we discuss the min-max strategy for the attacker in the worst-case scenario. In this subsection, we will discuss how the attacker can further reduce the risk using additive white Gaussian noise (AWGN).

Suppose that after performing intracopy and intercopy attack, the attacker introduces AWGN to the colluded copy to further reduce the risk of being detected. Then, the attack problem can be formulated as

$$\hat{f}(t) = \sum_{k=1}^{M}\frac{1}{M}\left[\sum_{i=-n}^{n}a_i f_k(t+i)\right] + \mathbf{N} \tag{34}$$

where $\mathbf{N}$ is AWGN with zero mean and σ^2 variance, i.e., $\mathbf{N} \sim N(0,\sigma^2)$.

$$\begin{aligned} \min_{\mathbf{a}_a} \quad & R(\mathbf{a}_d^\star) = \min_{\mathbf{a}_a}\max_{\mathbf{a}_d} Q\left(\frac{Q^{-1}(\alpha)||\Lambda\mathbf{a}_a||_2 - \frac{1}{M}E\left[\frac{\mathbf{a}_d{}^T\mathbf{W}_k^T\mathbf{W}_k\mathbf{a}_a}{||\mathbf{W}_k\mathbf{a}_d||_2}\right]}{||\Lambda\mathbf{a}_a||_2}\right) \\ s.t. \quad & D = \mathbf{a}_a{}^T\mathbf{K}\mathbf{a}_a \le D_0 \\ & \mathbf{1}^T\mathbf{a}_a = 1. \end{aligned} \tag{31}$$

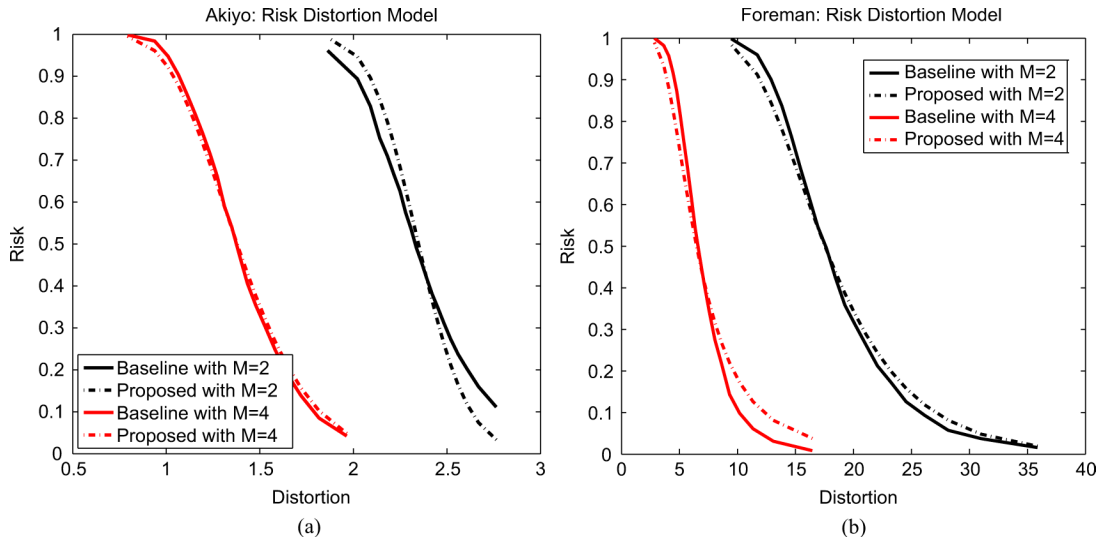

Fig. 3. Risk-distortion model for Akiyo and Foreman sequences: (a) Akiyo and (b) Foreman.

In the worst case scenario, similar to (28), the detection statistics can be computed by

$$TN_k''''(t) = \frac{\mathbf{a}^T\mathbf{W}_k^T\left(\mathbf{e}_I + \frac{1}{M}\sum_{i=1}^{M}\mathbf{W}_i + \mathbf{N}\right)\mathbf{a}}{\|\mathbf{W}_k\mathbf{a}\|_2}. \quad (35)$$

Similar to the analysis in the previous subsection, we can find the min-max strategy iteratively by solving the following optimization problem:

$$\begin{aligned} \min_{\mathbf{a}^{(t)}} \quad & \|\mathbf{W}_k\mathbf{a}^{(t)}\|_2^2 - \xi^{(t)}(\|\Lambda\mathbf{a}^{(t)}\|_2^2 + \sigma^2) \\ s.t. \quad & D = {\mathbf{a}^{(t)}}^T\mathbf{K}\mathbf{a}^{(t)} \le D_0 \\ & \mathbf{1}^T\mathbf{a}^{(t)} = 1 \end{aligned} \quad (36)$$

with $\xi^{(t+1)} = \|\mathbf{W}_k\mathbf{a}^{(t)}\|_2^2/\|\Lambda\mathbf{a}^{(t)}\|_2^2 + \sigma^2$. Note that since $\xi^{(t)} > 0$, we need to use CCCP to find the locally optimal solution.

VI. Parameter Estimation

From Sections IV and V, we can see that the risk-distortion relationship is determined by three parameters $\mathbf{p}$, $\mathbf{W}_k^T\mathbf{W}_k$, and $\mathbf{K}$. Now, we introduce in details how to estimate these three parameters. Since the attackers do not know the information about the original source signal $I(t)$ and the fingerprint signal $W_k(t)$. Instead, what they have is the fingerprinted signal $f_k(t-n),\ldots,f_k(t+n)$. In order to obtain the risk-distortion relationship, we need to first estimate the parameters $\mathbf{p}$, $\mathbf{W}_k^T\mathbf{W}_k$, and $\mathbf{K}$ based upon $f_k(t-n),\ldots,f_k(t+n)$.

Let $\mathbf{f}_k = [f_k(t-n),\ldots,f_k(t+n)]$. From (1), we can see that the fingerprinted signal is the sum of the original signal and the fingerprint, base on which the difference between $\mathbf{f}_k$ and its smooth version among all the colluders can be expressed as

$$\mathbf{f}_k - \frac{1}{M}\sum_{i=1}^{M}\mathbf{f}_i = \frac{M-1}{M}\mathbf{W}_k - \frac{1}{M}\sum_{i=1,i\neq k}^{M}\mathbf{W}_i \quad (37)$$

which means that we can use the fingerprinted signal $\mathbf{f}_k$ to compute the correlation matrix of the fingerprint signal $\mathbf{W}_k$ by

$$\begin{aligned} &E[\mathbf{W}_k^T\mathbf{W}_k] \\ &= \frac{1}{M-1}\sum_{j=1}^{M}E\left[\mathbf{f}_j - \frac{1}{M}\sum_{i=1}^{M}\mathbf{f}_i\right]^T\left[\mathbf{f}_j - \frac{1}{M}\sum_{i=1}^{M}\mathbf{f}_i\right]. \end{aligned} \quad (38)$$

The parameter $\mathbf{p}$ can be estimated using

$$\mathbf{p}(i) = \frac{E[\mathbf{W}_k^T\mathbf{W}_k]_{i,n}}{\sqrt{\frac{1}{2n+1}\sum_{j=1}^{2n+1}E[\mathbf{W}_k^T\mathbf{W}_k]_{j,j}}} \quad (39)$$

where $E[\mathbf{W}_k^T\mathbf{W}_k]_{i,j}$ is the i^{th} row and j^{th} column element of $E[\mathbf{W}_k^T\mathbf{W}_k]$.

In order to estimate the parameter $\mathbf{K}$, we need to first estimate $E[\mathbf{e}_I^T\mathbf{e}_I]$ using $\mathbf{f}_k$ as shown in (40) at the bottom of the next page.

VII. Experimental Results

To evaluate the proposed risk-distortion model, we conduct the experiments on real video data. Two video sequences (Akiyo, Foreman) in QCIF format are tested. We use the human visual model based spread spectrum embedding [1], and embed the fingerprint in the DCT domain. We generate independent vectors (length-N, with $N = 176 \times 144$) from Gaussian distribution $N(0,1)$, and then apply Gram-Schmidt orthogonalization to produce fingerprint strictly satisfying $E[W_i(t)^T W_j(t)] = \delta_{i,j}$. Then, we scale the fingerprint to let

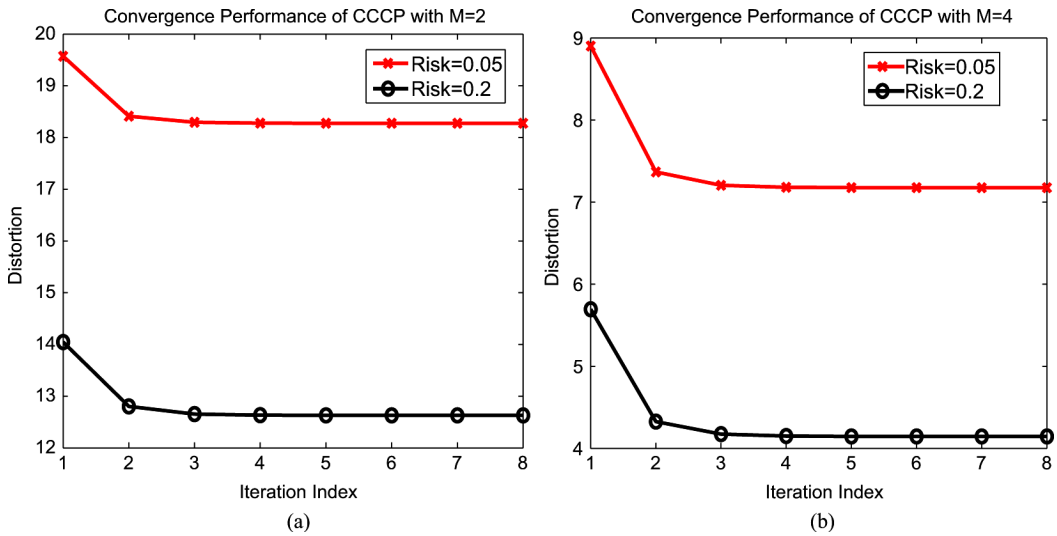

Fig. 4. Convergence performance of CCCP: (a) $\mathrm{M} = 2$ and (b) $\mathrm{M} = 4$.

the variance be σ_w^2, followed by the inverse Gram-Schmidt orthogonalization to ensure the fingerprint of each user satisfy (2) strictly with $\gamma = 0.5$. We assume that the collusion attacks are also in the DCT domain. At the detector's side, a nonblind detection is performed where the host signal is first removed from the colluded copy. And the detector uses the correlation-based detection statistics to identify the attackers. In all the following experiments, the parameter n is set to be 5, which means that the 10 temporally adjacent frames are involved in the intracopy attack process for each attacker. The false alarm probability is set to be $\alpha = 10^{-4}$.

We first evaluate the accuracy of the proposed risk distortion model by comparing with the baseline curve, which is the experimental risk-distortion curve. Here, the experimental risk is defined as the average positive detection probability by averaging over 400 runs of simulation. For each video sequence, the number of attackers $M = 2$ and $M = 4$ are tested. As shown in Fig. 3, the risk-distortion curve derived by the proposed model coincides with the baseline curve with small mismatch for both sequences, which demonstrates the effectiveness of the proposed risk-distortion model. Note that the mismatch mainly comes from the model error for the residue and the parameter estimation error. In the rest of this paper, we denote the risk-distortion curve obtained by our model as "***Absolute Risk Distortion Curve***."

The convergence performances of the CCCP process are shown in Fig. 4. From Fig. 4, we can see that with CCCP, for any fixed risk constraint, the distortion converges in a few iterations (less than 8 in the examples). Note that due to page limitation, we only show the cases when risk is fixed at 0.05 and 0.2. Similar behaviors are observed for different risk constraints.

We then study the risk distortion curve when the side information is available, which we denote as "***Relative Risk Distortion Curve***." In such a case, the optimal strategy for the attacker or detector lies on his/her opponent's strategy. Based upon the action that the opponent took, the attackers or detector can choose the best response using (21) or (27). In Fig. 5, we show the result of the "***Absolute Risk Distortion Curve***" and "***Relative Risk Distortion Curve***." We start with the "***Absolute Risk Distortion Curve***," which is obtained using (14). Then, if the detector has the perfect knowledge of the attackers' strategy and choose his/her optimal strategy based upon the side information. The resulting risk distortion curve is denoted as "***Relative Risk Distortion Curve Stage 1***." On the other hand, if the attackers know that the detector uses the side information of the attacker in previous stage, they will change their optimal strategy accordingly. The resulting risk distortion curve is denoted as "***Relative Risk Distortion Curve Stage 2***." We repeat these detection and attack process until stage 5. As shown in Fig. 5, when the detector has the perfect side information of the attackers' strategy, the risk of the attackers to be detected increases and the risk distortion curve moves up in the red arrow direction. On the other hand, if the attackers have the perfect side information of the detector's strategy, the risk of the attackers to be detected decreases and the risk distortion curve moves down in the blue arrow direc-

$$\begin{aligned} E[\mathbf{e}_I^T \mathbf{e}_I]_{i,j} &= E[I(t-n+i) - I(t)]^T [I(t-n+j) - I(t)] \\ &= E[f_k(t-n+i)^T f_k(t-n+j)] - E[f_k(t-n+j)^T f_k(t)] \\ &\quad - E[f_k(t-n+i)^T f_k(t)] + E[f_k(t)^T f_k(t)] - E[\mathbf{W}_k^T \mathbf{W}_k]_{i,j} \\ &\quad + E[\mathbf{W}_k^T \mathbf{W}_k]_{i,n} + E[\mathbf{W}_k^T \mathbf{W}_k]_{j,n} - E[\mathbf{W}_k^T \mathbf{W}_k]_{n,n}. \end{aligned} \tag{40}$$

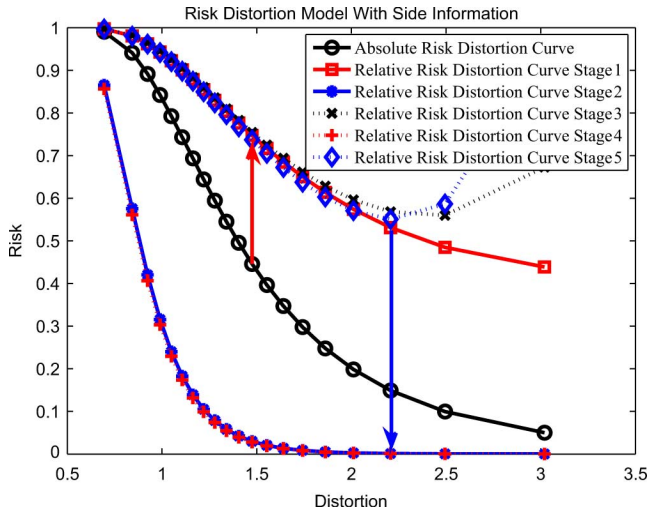

Fig. 5. "*Absolute Risk Distortion Curve*" and "*Relative Risk Distortion Curve*."

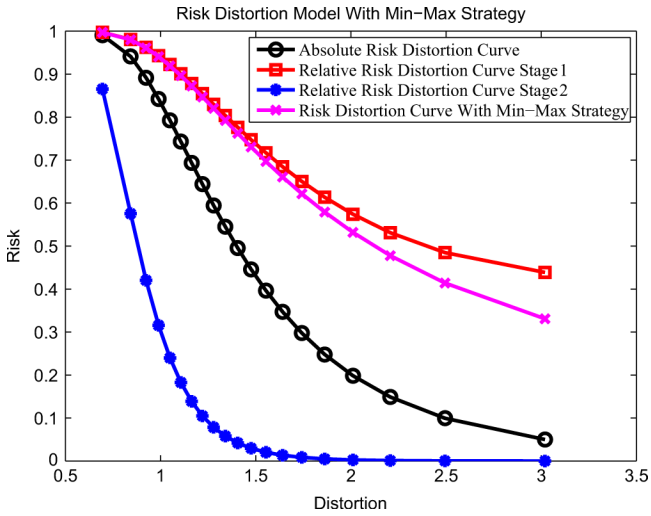

Fig. 6. Risk distortion curve with min-max strategy.

tion. This phenomenon shows the importance of the side information. The one who has the perfect side information of his/her opponent will lead the game and pull the risk distortion curve along the direction that benefits him/her.

Moreover, from Fig. 5, we can see that when the distortion is larger than 2.5, the "***Relative Risk Distortion Curve Stage 3***" curve and "***Relative Risk Distortion Curve Stage 5***" curve increase as the distortion increases. This phenomenon is partly because only the locally optimal solution is found using CCCP when the optimization problem in (27) is nonconvex.

In reality, the attackers need to choose his/her strategy first. In case of "naive" detector with fixed strategy, if the attackers know the perfect side information of the detector, they can choose their optimal strategy based upon the side information. On the other hand, if the detector is a powerful detector who can always estimate the attackers' strategy, the best strategy for the attackers is to minimize the risk of the worst case scenario, i.e., the min-max strategy. In Fig. 6, we show the risk distortion curve with min-max strategy. We can see that although the risk distortion curve with min-max strategy achieves the lowest risk among all the cases that the detector has the perfect side information, there is a big risk gap compared with the "***Absolute Risk Distortion Curve***."

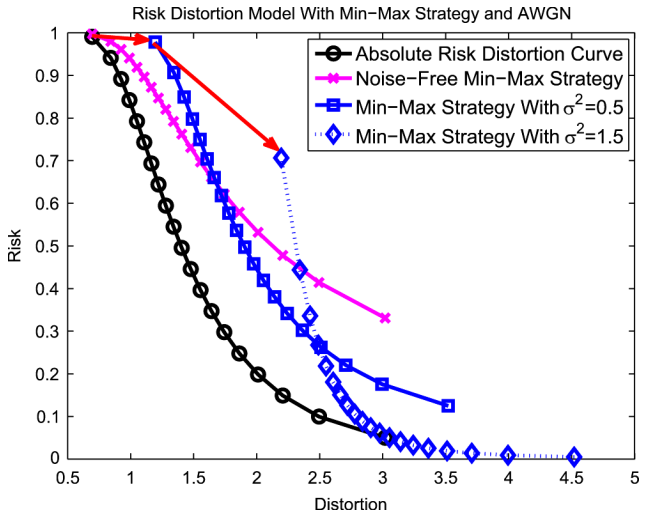

Fig. 7. Risk distortion curve with min-max strategy and AWGN.

In Fig. 7, we show the risk distortion curves with min-max strategy and AWGN. We can see that as the noise variance increases, the risk distortion curve moves along the red arrow direction. This is because when the noise variance increases, the distortion increases but the risk decreases. We can also see that when the noise variance is equal to 1.5, the risk distortion curve with min-max strategy meets the "***Absolute Risk Distortion Curve***" for all distortions larger than 3. Therefore, with a proper noise variance, we can reach the "***Absolute Risk Distortion Curve***" even with the min-max strategy.

VIII. Conclusion

In this paper, we provided a theoretical analysis on the risk-distortion relationship for the linear video collusion attack with Gaussian fingerprint, and conducted several experiments on real video sequences to verify the proposed risk-distortion model. From the experimental results, we could see that if the attackers have the perfect knowledge of the detector's strategy, they can choose the corresponding optimal strategy to destroy the fingerprint with a small distortion. However, if the detector is so powerful that can always estimate the attackers' strategy, the best strategy for the attacker is the min-max strategy. Moreover, we show that the attackers can further reduce the risk of being detected by introducing AWGN with a cost of larger distortion.

References

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

[2] M. Wu, W. Trappe, Z. J. Wang, and R. Liu, "Collusion-resistant fingerprinting for multimedia," *IEEE Signal Process. Mag.*, vol. 21, no. 2, pp. 15–27, Mar. 2004.

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

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

[5] H. Stone, Analysis of Attacks on Image Watermarks with Randomized Coefficients NEC Research Inst. Tech. Report, 1996.
[6] H. V. Zhao, M. Wu, Z. J. Wang, and K. J. R. Liu, "Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting," *IEEE Trans. Image Process.*, vol. 14, no. 5, pp. 646–661, May 2005.
[7] A. L. Varna, S. He, A. Swaminathan, and M. Wu, "Analysis of nonlinear collusion attacks on fingerprinting systems for compressed multimedia," in *Proc. IEEE Int. Conf. Image Processing*, San Antonio, TX, 2007, pp. 133–136.
[8] Y. Wu, "Nonlinear collusion attack on a watermarking scheme for buyer authentication," *IEEE Trans. Multimedia*, vol. 8, no. 3, pp. 626–629, Jun. 2006.
[9] J. Su, J. Eggers, and B. Girod, "Capacity of digital watermarks subject to an optimal collusion attacks," presented at the Proc. Eur. Signal Processing Conf., 2000.
[10] H. Zhao and K. J. R. Liu, "Traitor-within-traitor behavior forensics: Strategy and risk minimization," *IEEE Trans. Inf Forensics Security*, vol. 1, no. 4, pp. 440–456, Dec. 2006.
[11] 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.
[12] 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.
[13] K. Su, D. Kundur, and D. Hatzinakos, "Spatially localized image-dependent watermarking for statistical invisibility and collusion resistance," *IEEE Trans. Multimedia*, vol. 7, no. 1, pp. 52–66, Feb. 2005.
[14] T. Chiang and Y. Q. Zhang, "A new rate control scheme using quadratic distortion model," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 7, no. 1, pp. 246–250, Feb. 1997.
[15] M. Dai, D. Loguinov, and H. Radha, "Analysis and distortion modeling of MPEG-4 FGS," in *Proc. IEEE Int. Conf. Image Processing*, College Station, TX, 2003, pp. 301–304.
[16] H. V. Poor, *An Introduction to Signal Detection and Estimation*, 2nd ed. New York: Springer-Verlag, 1999.
[17] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[18] P.-M Cheung and J. T. Kwok, "A regularization framework for multiple-instance learning," in *Proc. Int. Conf. Machine Learning*, 2006, pp. 193–2000.
[19] A. Smola, S. Vishwanathan, and T. Hofmann, "Kernel methods for missing variables," in *Proc. Int. Workshop Artificial Intelligence and Statistics*, 2005, pp. 325–332.

Yan Chen (S'06) received the B.S. degree from the University of Science and Technology of China (USTC), Hefei, China, in 2004, the M.Phil degree from Hong Kong University of Science and Technology (HKUST), Kowloon, Hong Kong, in 2007, and is currently pursuing the Ph.D. degree in the Department of Electrical and Computer Engineering at University of Maryland, College Park.

His current research interests are in game theoretical modelling for multimedia social networks, multimedia signal processing, cooperative multimedia communication and networking, and multimedia forensic. He received the University of Maryland Future Faculty Fellowship in 2010.

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

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

K. J. Ray Liu (F'03) is a Distinguished Scholar-Teacher of University of Maryland, College Park. He is Associate Chair of Graduate Studies and Research of Electrical and Computer Engineering Department and leads the Maryland Signals and Information Group conducting research encompassing broad aspects of wireless communications and networking, information forensics and security, multimedia signal processing, and biomedical engineering. He is the recipient of numerous honors and awards including IEEE Signal Processing Society Technical Achievement Award and Distinguished Lecturer. He also received various teaching and research recognitions from University of Maryland including university-level Invention of the Year Award; and Poole and Kent Senior Faculty Teaching Award and Outstanding Faculty Research Award, both from A. James Clark School of Engineering. Dr. Liu is a Fellow of IEEE and AAAS.

Dr. Liu is President-Elect and was Vice President—Publications of IEEE Signal Processing Society. He was the Editor-in-Chief of IEEE SIGNAL PROCESSING MAGAZINE and the founding Editor-in-Chief of *EURASIP Journal on Advances in Signal Processing*. His recent books include *Cognitive Radio Networking and Security: A Game Theoretical View*, Cambridge University Press, 2010; *Cooperative Communications and Networking*, Cambridge University Press, 2008; *Resource Allocation for Wireless Networks: Basics, Techniques, and Applications*, Cambridge University Press, 2008; *Ultra-Wideband Communication Systems: The Multiband OFDM Approach*, IEEE-Wiley, 2007; *Network-Aware Security for Group Communications*, Springer, 2007; *Multimedia Fingerprinting Forensics for Traitor Tracing*, Hindawi, 2005; *Handbook on Array Processing and Sensor Networks*, IEEE-Wiley, 2009.