Forensic Analysis of Nonlinear Collusion Attacks for Multimedia Fingerprinting

H. Vicky Zhao, *Member, IEEE*, Min Wu, *Member, IEEE*, Z. Jane Wang, *Member, IEEE*, and K. J. Ray Liu, *Fellow, IEEE*

Abstract—**Digital fingerprinting is a technology for tracing the distribution of multimedia content and protecting them from unauthorized redistribution. Unique identification information is embedded into each distributed copy of multimedia signal and serves as a digital fingerprint. Collusion attack is a cost-effective attack against digital fingerprinting, where colluders combine several copies with the same content but different fingerprints to remove or attenuate the original fingerprints. In this paper, we investigate the average collusion attack and several basic nonlinear collusions on independent Gaussian fingerprints, and study their effectiveness and the impact on the perceptual quality. With unbounded Gaussian fingerprints, perceivable distortion may exist in the fingerprinted copies as well as the copies after the collusion attacks. In order to remove this perceptual distortion, we introduce bounded Gaussian-like fingerprints and study their performance under collusion attacks. We also study several commonly used detection statistics and analyze their performance under collusion attacks. We further propose a preprocessing technique of the extracted fingerprints specifically for collusion scenarios to improve the detection performance.**

Index Terms—**Digital forensics, multimedia fingerprinting, nonlinear collusion attacks, spread spectrum embedding, traitor tracing.**

I. Introduction

WITH the rapid development of multimedia technologies and the wide deployment of broadband networks, an increasing amount of multimedia data are distributed through networks. This introduces an urgent need to protect the proper distribution and use of multimedia content, especially in view of the ease of copying and manipulating digital multimedia data.

Although traditional cryptography can provide multimedia data with desired security during transmission, the protection vanishes after the data are decrypted into clear text. Digital watermarking is one of the emerging technologies to address the protection of multimedia content after decryption [1]–[3], and digital fingerprinting is a specific application of digital watermarking to trace illegal redistribution of multimedia content, where unique identification information is embedded into each copy prior to distribution. *Collusion* is a cost-effective attack against digital fingerprinting, where several users (colluders) combine information from different copies and generate a new copy in which the original fingerprints are removed or attenuated [4], [5]. Digital fingerprints should not only be robust against common signal processing and single-copy attacks [6]–[8], but also be resistant to collusion attacks.

An early work on digital fingerprint code design and collusion attacks was proposed in [9], which assumed that the colluders can detect a specific fingerprint code bit if it takes different values between their fingerprinted copies and can change it to any value. For those bits where different copies have the same value, it was assumed that the colluders cannot change an undetected bit without rendering the object useless. Based on these assumptions, a fingerprint code of length $O(K^4 \log(M))$ was built to catch at least one colluder out of up to K total colluders with arbitrarily high probabilities, where M is the number of total users. Similar work was presented in [10], which focused on tracing the leakage of decryption keys in broadcast instead of tracing multimedia content.

In [11], improvement was made upon the fingerprint code in [9] by replacing the lower layer code with direct spread spectrum sequence. It relaxed the assumptions in [9] and increased the total number of users that can be supported by three times. In [12] and [13], new features were introduced in the fingerprint code, such as dynamic code design and asymmetric fingerprinting.

These prior works mainly concern fingerprint code design and address few issues on the actual fingerprint embedding and detection. Multimedia data have a unique characteristic that minor perturbations on the values will not introduce perceptually distinguishable difference. This robustness makes it feasible and desirable to embed fingerprints seamlessly into the host multimedia data. Fingerprint codes designed by these prior works are usually too long to be reliably embedded into and extracted from multimedia data. Furthermore, for generic data, colluders can easily detect a fingerprint code bit if it differs between different copies and change it to any value. However, for multimedia data such as images, the embedding is capable of spreading each fingerprint code bit over the entire content. Thus, different bits embedded additively over the same region are not distinguishable, neither can they be changed to any value due to the perceptual quality constraint. Consequently, the assumptions of the collusion attacks in many previous works are not always suitable for multimedia data. Instead, the average attack and those order statistics based nonlinear

Manuscript received November 26, 2002; revised May 12, 2004. This work was supported in part by the Air Force Research Laboratory under DDET Grant F30602-03-2-0045 and in part by the National Science Foundation under CAREER Award CCR-0133704. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Gopal Pingali.

H. V. Zhao, M. Wu, and K. J. R. Liu are with the Department of Electrical and Computer Engineering, Institute for Systems Research, University of Maryland, College Park, MD 20742 USA (e-mail: hzhao@eng.umd.edu; minwu@eng.umd.edu; kjrliu@eng.umd.edu).

Z. J. Wang is with the Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC V6T 1Z4 Canada (e-mail: zjanew@ece.ubc.ca).

Digital Object Identifier 10.1109/TIP.2005.846035

collusions in [4] are more common when colluding multimedia data.

In [14], a two-layer fingerprinting design scheme for multimedia data was proposed where the inner code from the spread spectrum embedding [15] is combined with an outer error-correcting code. In [16], the finite projective geometry was used to generate codes whose overlap with each other can identify colluding users. The Anti Collusion Code based on combinatorial theories was proposed in [5] for multimedia fingerprint code design. In [17], the collusion attack was modeled as averaging different copies followed by an additive noise, and $O(\sqrt{N/\log N})$ colluders were shown to be enough to break the fingerprint system where N is the fingerprint code length. Similar results were given in [18]. The collusion attack model was generalized to linear shift invariant filtering followed by an additive noise in [19].

Most works on digital fingerprinting and collusion attacks for multimedia employ the watermark embedding method in [15] and use a linear collusion attack model. In [4], several types of collusion attacks were studied, including a few nonlinear collusion attacks. For uniformly distributed fingerprints, nonlinear collusion attacks were shown to defeat the fingerprinting system more effectively than the average attack [4]. Simulation results in [4] also showed that normally distributed fingerprints are more robust against nonlinear collusion attacks than uniform fingerprints, but analytical study on the Gaussian fingerprints' performance was not provided. In addition to the robustness against collusion attacks, compared with discrete watermarks and uniform watermarks, Gaussian watermarks have the advantage that they do not provide the attackers with the positions and the amplitudes of the embedded watermarks under statistical and histogram attacks [20]. Therefore, we use in this paper Gaussian distributed fingerprints. We first consider from the colluders' point of view and compare various nonlinear collusion attacks on independent Gaussian fingerprints. We analyze the effectiveness of the collusion attacks and the perceptual quality of the colluded signals. We then shift our role to desinger/detector and analyze the performance of several commonly used detection statistics [4], [21], [22] in the literature under collusion attacks. There is no other work to our knowledge that compares their detection performance under collusion attacks. We use digital image as an example, and our results are applicable to other types of multimedia.

Note that, in addition to collusion attacks, the colluders can also apply single-copy attacks to further hinder the detection. Spread spectrum embedding [15], [23] has been widely used in the literature and is proven to be resistant to many single-copy attacks. Recent investigation has shown that simple rotation, scale and translation based geometric attacks may prevent the detection of the embedded watermarks [24]. However, since the host signal can be made available to the detector in digital fingerprinting applications, the detector can first register the attacked copy with respect to the host signal and undo the geometric attacks before the colluder identification process. It was shown in [25] that the alignment noise from inverting geometric distortions is generally very small and, therefore, will not significantly affect the detection performance. Consequently, in this paper, we focus on collusion attacks, which are effective and have not been well studied in the literature. Real systems should contain other components, e.g., the registration module, to combat possible distortions of other types.

The organization of this paper is as follows. We begin, in Section II, with a system model of digital fingerprinting and collusion attacks. Then, in Section III, we analyze the effectiveness and the perceptual quality of different nonlinear collusion attacks, and investigate the detection performance of different detection statistics. In Section IV, we first study the resistance of independent unbounded Gaussian fingerprints to different collusion attacks. We find that while Gaussian fingerprints are more robust against collusion attacks, they may introduce noticeable distortion in the fingerprinted copies due to their unbounded nature. In order to achieve both the robustness against collusion attacks and the imperceptibility, we introduce bounded Gaussian-like fingerprints and analyze their performance. In Section V, we propose a preprocessing technique of the extracted fingerprints to improve the detection performance. Section VI shows the simulation results on real images. A few more nonlinear collusion attacks are discussed in Section VII. Finally, conclusions are drawn in Section VIII.

II. System Model

A. System Model and Assumptions

We consider a digital fingerprinting and collusion attack system that consists of three parts: fingerprint embedding, collusion attacks, and fingerprint detection.

We use in this paper the spread spectrum embedding [15], [23] to hide fingerprints in the host signal. Assume that there are a total of M users in the system. Given a host signal represented by a vector $\mathbf{S}$ of length N, the owner generates a unique fingerprint $\mathbf{W}^{(i)}$ of length N for each user $\mathbf{u}^{(i)}$, $i = 1, 2, \ldots, M$. In this paper, we assume that the M fingerprints $\{\mathbf{W}^{(i)}\}_{i=1}^{M}$ are independent of each other. The fingerprinted copy $\mathbf{X}^{(i)}$ that is distributed to user $\mathbf{u}^{(i)}$ is generated by $\mathbf{X}_j^{(i)} = \mathbf{S}_j + \alpha_j \mathbf{W}_j^{(i)}$. Here, $\mathbf{X}_j^{(i)}$, $\mathbf{S}_j$, and $\mathbf{W}_j^{(i)}$ are the jth components of the fingerprinted copy, the original signal, and the fingerprint, respectively, and $\boldsymbol{\alpha}$ is the *just-noticeable-difference* (JND) from human visual models [23] to control the energy and achieve the imperceptibility of the embedded fingerprints. Then, the fingerprinted copy $\mathbf{X}^{(i)}$ is distributed to user $\mathbf{u}^{(i)}$.

Assume that K out of M users collude, and $S_C = \{i_1, i_2, \ldots, i_K\}$ is the set containing the indices of the colluders. We further assume that the collusion attack is in the same domain as the fingerprint embedding. With K different copies $\{\mathbf{X}^{(k)}\}_{k\in S_C}$, the colluders generate the jth component of the attacked copy V_j using one of the collusion functions shown in (1)

$$\begin{aligned}
\text{average attack}: &\quad V_j^{\text{ave}} = \sum_{k\in S_C} \frac{X_j^{(k)}}{K}\\
\text{minimum attack}: &\quad V_j^{\min} = \min\left(\{X_j^k\}_{k\in S_C}\right)\\
\text{maximum attack}: &\quad V_j^{\max} = \max\left(\{X_j^{(k)}\}_{k\in S_C}\right)
\end{aligned}$$

$$\begin{aligned}
\text{median attack}: \quad & V_j^{\text{med}} = \text{median}\left(\{X_j^{(k)}\}_{k\in S_C}\right)\\
\text{minmax attack}: \quad & V_j^{\text{minmax}} = \frac{(V_j^{\min}+V_j^{\max})}{2}\\
\text{modified negative attack}: \quad & \\
& V_j^{\text{ModNeg}} = V_j^{\min}+V_j^{\max}-V_j^{\text{med}}\\
\text{randomized negative attack}: \quad & \\
& V_j^{\text{randneg}} = \begin{cases} V_j^{\min} & \text{with prob. } p\\ V_j^{\max} & \text{with prob. } 1-p. \end{cases}
\end{aligned} \tag{1}$$

In (1), $\min\left(\{X_j^k\}_{k\in S_C}\right)$, $\max\left(\{X_j^k\}_{k\in S_C}\right)$ and $\text{median}\left(\{X_j^k\}_{k\in S_C}\right)$ return the minimum, the maximum and the median values of $\{X_j^k\}_{k\in S_C}$, respectively. The colluded copy is $\mathbf{V} = [V_1, V_2, \ldots, V_N]$. For our model, applying the collusion attacks to the fingerprinted copies is equivalent to applying the collusion attacks to the embedded fingerprints. For example

$$\begin{aligned}
\mathbf{V}_j^{\min} &= \min\left(\{\mathbf{S}_j + \boldsymbol{\alpha}\cdot\mathbf{W}_j^{(k)}\}_{k\in S_C}\right)\\
&= \mathbf{S}_j + \boldsymbol{\alpha}\cdot\min\left(\{\mathbf{W}_j^{(k)}\}_{k\in S_C}\right).
\end{aligned}$$

In fingerprinting applications, the original signal $\mathbf{S}$ is often available to detectors. To improve the detection performance [5], the detector first removes the host signal from the attacked copy and extracts the fingerprint $\mathbf{Y} = g(\{\mathbf{W}^{(k)}\}_{k\in S_C})$ where $g(\cdot)$ is a collusion function defined in (1). The detector analyzes the similarity between $\mathbf{Y}$ and each of the M original fingerprints $\{\mathbf{W}^{(i)}\}$, and outputs the estimated colluder set.

In the literature, there are three detection statistics available to test the presence of the original fingerprint $\mathbf{W}^{(i)}$ in the extracted fingerprint $\mathbf{Y}$ [4], [21], [22]

$$\begin{aligned}
T_N^{(i)} &= \frac{\langle \mathbf{Y}, \mathbf{W}^{(i)}\rangle}{\sqrt{\|\mathbf{W}^{(i)}\|^2}}\\
Z^{(i)} &= \frac{1}{2}\sqrt{N-3}\log\frac{1+\rho^{(i)}}{1-\rho^{(i)}} \text{ where}\\
\rho^{(i)} &= \frac{\frac{1}{N}\sum_{j=1}^{N} Y_j W_j^{(i)} - \widetilde{Y}\cdot\widetilde{W}^{(i)}}{\sqrt{\hat{\sigma}_W^2\hat{\sigma}_Y^2}}, \text{ and}\\
q^{(i)} &= \frac{\sqrt{N}M_y}{\sqrt{V_y^2}}, \text{ where}\\
M_y &= \sum_{j=1}^{N}\frac{Y_j W_j^{(i)}}{N} \text{ and } V_y^2 = \sum_{j=1}^{N}\frac{(Y_j W_j^{(i)} - M_y)^2}{N-1}.
\end{aligned} \tag{2}$$

In (2), $\|\mathbf{W}^{(i)}\|$ is the Euclidean norm of $\mathbf{W}^{(i)}$; N is the length of the fingerprint; $\rho^{(i)}$ is the estimated correlation coefficient between $\mathbf{Y}$ and $\mathbf{W}^{(i)}$; $\widetilde{Y} = (1/N)\sum_{j=1}^{N} Y_j$ and $\widetilde{W}^{(i)} = (1/N)\sum_{j=1}^{N} W_j^{(i)}$ are the sample means of $\mathbf{Y}$ and $\mathbf{W}^{(i)}$, respectively; $\hat{\sigma}_W^2 = (1/(N-1))\sum_j (W_j^{(i)} - \widetilde{W}^{(i)})$ and $\hat{\sigma}_Y^2 = (1/(N-1))\sum_j (Y_j - \widetilde{Y})$ are the unbiased estimates of the original fingerprint's variance and the extracted fingerprint's variance, respectively; and M_y and V_y^2 are the sample mean and sample variance of $\{Y_j W_j^{(i)}\}$. Note that all three detection statistics are correlation based in which the correlation between the extracted fingerprint $\mathbf{Y}$ and the original fingerprint $\mathbf{W}^{(i)}$ is the kernel term, and they differ primarily in the way of normalization.

B. Performance Criteria

In this paper, we consider the following performance criteria to analyze different collusion attacks and different detection statistics.

1) Effectiveness of Collusion Attacks and Detection Performance of Detection Statistics: To study the effectiveness of collusion attacks and the performance of detection statistics, different criteria were used to address different applications in the literature. One set of criteria is the probability of falsely accusing at least one innocent user and the probability of not identifying any of the colluders [17], [18]. The second set of criteria is the fraction of colluders that are successfully captured and the fraction of innocent users that are falsely accused, as considered in [5] and [26]. In this paper, we adopt these criteria and use the following measurements:

- P_d: probability of capturing at least one colluder;
- P_{fp}: probability of falsely accusing at least one innocent user;
- F_d: fraction of colluders that are successfully captured;
- F_{fp}: fraction of innocent users that are falsely accused.

Different applications have different goals and may need different balance between capturing colluders and accusing innocent users. P_d and P_{fp} are used in applications where falsely accusing an innocent user may lead to severe consequences. One possible application is to provide digital evidence in the court of law. The detector in these applications is designed to capture one colluder with high confidence. On the other hand, F_d and F_{fp} are used in applications where the detection process is combined with other components in the decision making system and other evidences to make the final decision. The detector there is designed to capture more colluders at the cost of accusing more innocent users.

2) Perceptual Quality: When considering the perceptual quality, one of the commonly used objective measurements on perceptual distortion is the mean square error (MSE) and equivalently PSNR for image applications. A major weakness of MSE is that it ignores the unique characteristic of multimedia data: minor perturbations on the data values will not cause noticeable distortion as long as they do not exceed the *just-noticeable difference* [23]. Furthermore, MSE only measures the average energy of the noise introduced and does not consider the local constraints on each noise component.

We take JND into consideration and define the following two new measurements:

- $F_{\text{JND}} \triangleq \sum_{j=1}^{N} I_{[|n_j|>\text{JND}_j]}/N$;
- the redefined mean square error $\text{MSE}_{\text{JND}} \triangleq \sum_{j=1}^{N} n_j'^2$ where n_j' is defined as

$$n_j' = \begin{cases} n_j + \text{JND}_j, & \text{if } n_j < -\text{JND}_j\\ 0, & \text{if } -\text{JND}_j \le n_j \le \text{JND}_j\\ n_j - \text{JND}_j, & \text{if } n_j > \text{JND}_j. \end{cases} \tag{3}$$

MSE_{JND} calculates the power of the noise components that introduce perceptual distortion and F_{JND} reflects the percentage of the noise components that exceed JND. A large MSE_{JND} or a large F_{JND} indicates large perceptual distortion introduced.

III. Statistical Analysis of Collusion Attacks and Detection Statistics

In this section, we will analyze the statistical behavior of three detection statistics under different collusion attacks.

A. Analysis of the Correlation Term Under Different Collusion Attacks

In our system model, the extracted fingerprint is $\mathbf{Y} = g\left(\{\mathbf{W}^{(k)}\}_{k\in S_C}\right)$. As discussed in the previous section, when measuring the similarity between $\mathbf{Y}$ and $\mathbf{W}^{(i)}$, all three statistics are correlation based, and the common kernel term is the linear correlation

$$\begin{aligned} T_N'^{(i)} &\triangleq \frac{1}{N}\langle \mathbf{Y}, \mathbf{W}^{(i)}\rangle \\ &= \frac{1}{N}\sum_{j=1}^{N} g(\{W_j^{(k)}\}_{k\in S_c})W_j^{(i)} \end{aligned} \tag{4}$$

where N is the length of the fingerprint. For different collusion attacks, $T_N'^{(i)}$ follows different distributions. This section analyzes the statistical behavior of this correlation term under different collusion attacks.

Under the assumption that $\{W_j^{(k)}, k = 1, \ldots, M\}_{j=1}^{N}$ are i.i.d. distributed with zero mean and variance σ_W^2, $\{g(\{W_j^{(k)}\}_{k\in S_c})W_j^{(i)}\}_{j=1}^{N}$ are also i.i.d. distributed. From central limit theorem, if $\{g(\{W_j^{(k)}\}_{k\in S_c})W_j^{(i)}\}_{j=1}^{N}$ have finite mean $\mu_{T_N'^{(i)}}$ and finite variance $\sigma^2_{T_N'^{(i)}}$, then $T_N'^{(i)}$ can be approximated by

$$T_N'^{(i)} \sim \mathcal{N}\left(\mu_{T_N'^{(i)}}, \frac{\sigma^2_{T_N'^{(i)}}}{N}\right). \tag{5}$$

The problem is reduced to find $\mu_{T_N'^{(i)}} = E\left[g(\{W^{(k)}\}_{k\in S_c})W^{(i)}\right]$ and $\sigma^2_{T_N'^{(i)}} = var\left[g(\{W^{(k)}\}_{k\in S_c})W^{(i)}\right]$. We simplify the notation by dropping the subscript j. For a given K and a given collusion function $g(\cdot)$, due to the symmetry of $g(\{W^{(k)}\}_{k\in S_c})W^{(i)}$ with respect to the user index i, all $g(\{W^{(k)}\}_{k\in S_c})W^{(i)}$ where $i \in S_C$ have the same mean and variance, and similarly, all $g(\{W^{(k)}\}_{k\in S_c})W^{(i)}$ where $i \notin S_C$ have the same mean and variance.

For $i \in S_C$, define

$$\begin{aligned} \mu_{g,H_1} &\triangleq E\left[g(\{W^{(k)}\}_{k\in S_c})W^{(i)}\right] \\ \text{and } \sigma^2_{g,H_1} &\triangleq var\left[g(\{W^{(k)}\}_{k\in S_c})W^{(i)}\right] \\ &= E\left[\left(g(\{W^{(k)}\}_{k\in S_c})W^{(i)}\right)^2\right] - (\mu_{g,H_1})^2. \end{aligned} \tag{6}$$

For $i \notin S_C$, because $\{W^{(i)}\}_{i=1}^{M}$ are i.i.d. distributed with zero mean and variance σ_W^2, we have

$$\begin{aligned} \mu_{g,H_0} &\triangleq E\left[g(\{W^{(k)}\}_{k\in S_c})W^{(i)}\right] = 0 \\ \text{and } \sigma^2_{g,H_0} &\triangleq var\left[g(\{W^{(k)}\}_{k\in S_c})W^{(i)}\right] \\ &= E\left[\left(g(\{W^{(k)}\}_{k\in S_c})\right)^2\right]\sigma_W^2. \end{aligned} \tag{7}$$

Therefore, $E\left[g(\{W^{(k)}\}_{k\in S_c})W^{(i)}\right]$, $E\left[\left(g(\{W^{(k)}\}_{k\in S_c})W^{(i)}\right)^2\right]$ for $i \in S_C$ and $E\left[\left(g(\{W^{(k)}\}_{k\in S_c})\right)^2\right]$ are needed for analyzing the correlation term under each collusion attack.

Under the average attack, if $i \in S_C$, we have

$$\begin{aligned} E\left[\left(\frac{1}{K}\sum_{k\in S_C} W^{(k)}\right)W^{(i)}\right] &= \frac{1}{K}\sigma_W^2 \\ E\left[\left(\frac{1}{K}\sum_{k\in S_C} W^{(k)}W^{(i)}\right)^2\right] &= \frac{1}{K^2}E\left[\left(W^{(i)}\right)^4\right] \\ &\quad + \frac{K-1}{K^2}\sigma_W^4 \\ \text{and } E\left[\left(\frac{1}{K}\sum_{k\in S_C} W^{(k)}\right)^2\right] &= \frac{1}{K}\sigma_W^2. \end{aligned} \tag{8}$$

Under the minimum attack, given the pdf and cdf of $W^{(i)}$, if the number of colluders is K, from the probability and order statistics theory [27], we can get the pdf of $W^{\min} \triangleq \min\left(\{W^{(k)}\}_{k\in S_C}\right)$

$$f_{W^{\min}}(W^{\min} = w') = Kf(w')[1 - F(w')]^{K-1}. \tag{9}$$

From (9), we can calculate the second moment of $W^{\min}$. For $i \in S_C$, we can express the joint pdf of $W^{\min}$ and $W^{(i)}$ as follows by noticing that $f_{W^{\min},W^{(i)}}(w', w)$ breaks into two nonzero regions

$$\begin{aligned} &f_{W^{\min},W^{(i)}}(W^{\min} = w', W^{(i)} = w) \\ &= \begin{cases} f(w')[1 - F(w')]^{K-1}, & \text{if } W^{\min} = W^{(i)} \\ (K-1)f(w')f(w)[1 - F(w')]^{K-2}, & \text{if } W^{\min} < W^{(i)}. \end{cases} \end{aligned} \tag{10}$$

Consequently, $E\left[W^{\min}W^{(i)}\right] = E\left[W^{\min}W^{(i)}\right]_1 + E\left[W^{\min}W^{(i)}\right]_2$, where

$$\begin{aligned} &E\left[W^{\min}W^{(i)}\right]_1 \\ &= \int_{-\infty}^{\infty} w'^2 f(w')[1 - F(w')]^{K-1}dw' \text{ and} \\ &E[W^{\min}W^{(i)}]_2 \\ &= \int_{-\infty}^{\infty} w'(K-1)f(w')[1-F(w')]^{K-2} \times \left(\int_{w'}^{\infty} wf(w)dw\right)dw'. \end{aligned} \tag{11}$$

The calculation of $E\left[\left(W^{\min}W^{(i)}\right)^2\right]$ is similar.

The analysis of the maximum and median attacks follows the same approach. For the maximum attack, the pdf of $W^{\max} \triangleq \max\left(\{W^{(k)}\}_{k\in S_C}\right)$ is

$$f_{W^{\max}}(W^{\max} = w') = Kf(w')F^{K-1}(w') \tag{12}$$

and the joint pdf of $W^{\max}$ and $W^{(i)}$ for $i \in S_C$ is

$$\begin{aligned} &f_{W^{\max},W^{(i)}}(W^{\max} = w', W^{(i)} = w) \\ &= \begin{cases} f(w')F^{K-1}(w'), & \text{if } W^{\max} = W^{(i)} \\ (K-1)f(w')f(w)F^{K-2}(w'), & \text{if } W^{\max} > W^{(i)}. \end{cases} \end{aligned} \tag{13}$$

Under the median attack, define $W^{\text{med}} \triangleq \text{median}\left(\{W^{(k)}\}_{k\in S_C}\right)$. If $K = 2l+1$, the pdf of W^{med} is

$$f_{W^{\text{med}}}(W^{\text{med}} = w') = K\binom{2l}{l} f(w')F^l(w')[1-F(w')]^l \tag{14}$$

and the joint pdf of W^{med} and $W^{(i)}$ for $i \in S_C$ is shown in (15), at the bottom of the page.

Under the minmax attack $W^{\text{minmax}} \triangleq (1/2)\left(W^{\min} + W^{\max}\right)$, if $i \in S_C$, we have

$$\begin{aligned} &E\left[W^{\text{minmax}}W^{(i)}\right] \\ &\quad= \frac{\left(E\left[W^{\min}W^{(i)}\right] + E\left[W^{\max}W^{(i)}\right]\right)}{2}, \\ &E\left[\left(W^{\text{minmax}}W^{(i)}\right)^2\right] \\ &\quad= \frac{\left\{E\left[\left(W^{\min}W^{(i)}\right)^2\right] + E\left[\left(W^{\max}W^{(i)}\right)^2\right]\right\}}{4} \\ &\quad\quad+ \frac{E\left[W^{\min}W^{\max}\left(W^{(i)}\right)^2\right]}{2}, \\ \text{and } &E\left[\left(W^{\text{minmax}}\right)^2\right] \\ &\quad= \frac{\left\{E\left[\left(W^{\min}\right)^2\right] + E\left[\left(W^{\max}\right)^2\right]\right\}}{4} \\ &\quad\quad+ \frac{E\left[W^{\min}W^{\max}\right]}{2} \end{aligned} \tag{16}$$

The results from the previous analysis on the minimum and the maximum attacks can be applied to (16). In addition, we can find the correlation between $W^{\min}$ and $W^{\max}$ from their joint pdf

$$\begin{aligned} &f_{W^{\min},W^{\max}}(W^{\min} = w', W^{\max} = w'') \\ &\quad= K(K-1)f(w')f(w'')[F(w'')-F(w')]^{K-2} \end{aligned} \tag{17}$$

$$\begin{aligned} &\text{thus } E\left[W^{\min}\cdot W^{\max}\right] \\ &\quad= \int_{-\infty}^{\infty}\int_{w'}^{\infty} w'w'' f_{W^{\min},W^{\max}}(w',w'')dw''dw'. \end{aligned} \tag{18}$$

The calculation of $E\left[\left(W^{\min}W^{\max}\right)^2\right]$ is similar. $E\left[W^{\min}W^{\max}\left(W^{(i)}\right)^2\right]$ is obtained based on the joint pdf of $W^{\min}, W^{\max}$, and $W^{(i)}$, which is shown in (19), at the bottom of the page.

The analysis of the modified negative (ModNeg) attack is similar to that of the minmax attack. If $K = 2l+1$, then the joint pdf of $W^{\min}$ and W^{med} and the joint pdf of W^{med} and $W^{\max}$ are

$$\begin{aligned} &f_{W^{\min},W^{\text{med}}}(W^{\min}=w', W^{\text{med}}=w'') \\ &\quad= (2l+1)2l\binom{2l-1}{l} f(w')f(w'') \\ &\quad\quad\times[F(w'')-F(w')]^{l-2}[1-F(w'')]^l \end{aligned} \tag{20}$$

and

$$\begin{aligned} &f_{W^{\text{med}},W^{\max}}(W^{\text{med}}=w', W^{\max}w'') \\ &\quad= (2l+1)2l\binom{2l-1}{l} f(w')f(w'') \\ &\quad\quad\times[F(w'')-F(w')]^{l-1}F^l(w'). \end{aligned} \tag{21}$$

For $i \in S_C$, the joint pdf of $W^{\min}, W^{\text{med}}$ and $W^{(i)}$ and the joint pdf of $W^{\max}$, W^{med}, and $W^{(i)}$ are shown in (22) and (23), respectively, at the bottom of the next page.

Under the randomized negative (RandNeg) attack, we assume that p is independent of $\{W^{(i)}\}$. The colluded fingerprint can be written as $W^{\text{randneg}} = W^{\min}\cdot B_p + W^{\max}\cdot(1-B_p)$, where B_p is a Bernoulli random variable with parameter p and is independent of $\{W^{(i)}\}$. The m-th moment $(m = 1, 2, \ldots)$ of $W^{\text{randneg}}W^{(i)}$ for $i \in S_C$ and the m-th moment of W^{randneg} are

$$\begin{aligned} E\left[\left(W^{\text{randneg}}W^{(i)}\right)^m\right] &= p\cdot E\left[\left(W^{\min}W^{(i)}\right)^m\right] \\ &\quad+ (1-p)\cdot E\left[\left(W^{\max}W^{(i)}\right)^m\right] \\ \text{and } E\left[\left(W^{\text{randneg}}\right)^m\right] &= p\cdot E\left[\left(W^{\min}\right)^m\right] \\ &\quad+ (1-p)\cdot E[(W^{\max})^m]. \end{aligned} \tag{24}$$

From all the above analysis, the correlation kernel term $T_N'^{(i)}$ can be approximated by the following Gaussian distribution

$$T_N'^{(i)} \sim \begin{cases} \mathcal{N}\left(0, \frac{\sigma^2_{g,H_0}}{N}\right), & \text{if } i \notin S_C \\ \mathcal{N}\left(\mu_{g,H_1}, \frac{\sigma^2_{g,H_1}}{N}\right), & \text{if } i \in S_C. \end{cases} \tag{25}$$

$$f_{W^{\text{med}},W^{(i)}}(W^{\text{med}} = w', W^{(i)} = w) = \begin{cases} \binom{2l}{l} f(w')F^l(w')[1-F(w')]^l, & \text{if } W_{\text{med}} = W^{(i)} \\ (K-1)\binom{2l-1}{l} f(w')f(w)F^l(w')[1-F(w')]^{l-1}, & \text{if } W^{\text{med}} < W^{(i)} \\ (K-1)\binom{2l-1}{l} f(w')f(w)F^{l-1}(w')[1-F(w')]^l, & \text{if } W^{\text{med}} > W^{(i)} \end{cases} \tag{15}$$

$$\begin{aligned} &f_{W^{\min},W^{\max},W^{(i)}}(W^{\min} = w', W^{\max} = w'', W^{(i)} = w) \\ &\quad= \begin{cases} (K-1)f(w')f(w'')[F(w'')-F(w')]^{K-2}, & \text{if } W^{\min} = W^{(i)} \\ (K-1)f(w')f(w'')[F(w'')-F(w')]^{K-2}, & \text{if } W^{\max} = W^{(i)} \\ (K-1)(K-2)f(w')f(w'')f(w)[F(w')-F(w'')]^{K-3}, & \text{if } W^{\min} < W^{(i)} < W^{\max}. \end{cases} \end{aligned} \tag{19}$$

B. Analysis of the Detection Statistics

From (25), we can approximate the detection statistics $T_N^{(i)}$ by a Gaussian random variable

$$T_N^{(i)} = \frac{NT_N^{\prime(i)}}{\sqrt{\|\mathbf{W}^i\|^2}} \sim \begin{cases} \mathcal{N}\left(0, \frac{\sigma_{g,H_0}^2}{\sigma_W^2}\right), & \text{if } i \notin S_C \\ \mathcal{N}\left(\frac{\sqrt{N}\mu_{g,H_1}}{\sigma_W}, \frac{\sigma_{g,H_1}^2}{\sigma_W^2}\right), & \text{if } i \in S_C. \end{cases} \tag{26}$$

The Z statistics can be approximated by a Gaussian random variable $\mathcal{N}(\mu_Z^{(i)}, 1)$ with mean $\mu_Z^{(i)} = (1/2)\sqrt{N-3}\log(1+E[\rho^{(i)}])/(1-E[\rho^{(i)}])$, where $E[\rho^{(i)}]$ is the mean of $\rho^{(i)}$ defined in (2) and is the estimated correlation coefficient of the extracted fingerprint $\mathbf{Y}$ and the original fingerprint $\mathbf{W}^{(i)}$ [4]. We can show that

$$Z^{(i)} \sim \begin{cases} \mathcal{N}(0,1), & \text{if } i \notin S_C \\ \mathcal{N}\left(\frac{1}{2}\sqrt{N-3}\log\frac{1+E[\rho^{(i)}]}{1-E[\rho^{(i)}]}, 1\right), & \text{if } i \in S_C. \end{cases} \tag{27}$$

Here, for $i \in S_C$

$$E[\rho^{(i)}] \approx \frac{cov\left[g(\{W^{(k)}\}_{k\in S_C}), W^{(i)}\right]}{\sqrt{\sigma_W^2\sigma_{g,Y}^2}} = \frac{\mu_{g,H_1}}{\sqrt{\sigma_W^2\sigma_{g,Y}^2}} \tag{28}$$

where $\sigma_{g,Y}^2$ is the variance of the extracted fingerprint.

The q statistics normalize the correlation term with the unbiased estimate of its variance. So we have

$$q^{(i)} \sim \begin{cases} \mathcal{N}(0,1), & \text{if } i \notin S_C \\ \mathcal{N}\left(\frac{\sqrt{N}\mu_{g,H_1}}{\sqrt{\sigma_{g,H_1}^2}}, 1\right), & \text{if } i \in S_C. \end{cases} \tag{29}$$

C. Analysis of the Performance of Collusion Attacks and Detection Statistics

1) Analysis of P_d, P_{fp}, $E[F_d]$, and $E[F_{fp}]$: In our system model with a total of M users and K colluders, given a signal to be tested and given one detection statistics, K out of the M statistics $\{T_N^{(i)}\}_{i=1}^M$ are normally distributed with a positive mean and the others are normally distributed with a zero mean, as analyzed in the previous section.

Take the T_N statistics as an example, define $\mu_1 \triangleq \sqrt{N}\mu_{g,H_1}/\sigma_W$, $\sigma_1^2 \triangleq \sigma_{g,H_1}^2/\sigma_W^2$, and $\sigma_0^2 \triangleq \sigma_{g,H_0}^2/\sigma_W^2$. If $\{T_N^{(i)}\}_{i=1}^M$ are uncorrelated with each other or the correlation is very small, then for a given threshold h, we can approximate P_d and P_{fp} by

$$P_d = P\left[\max_{i\in S_C} T_N^{(i)} > h\right] \approx 1 - \left[1 - Q\left(\frac{h-\mu_1}{\sigma_1}\right)\right]^K$$

and

$$P_{fp} = P\left[\max_{i\notin S_C} T_N^{(i)} > h\right] \approx 1 - \left[1 - Q\left(\frac{h}{\sigma_0}\right)\right]^{M-K} \tag{30}$$

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

To calculate $E[F_d]$ and $E[F_{fp}]$, we can have the following approximations:

$$E[F_d] = P\left[T_N^{(i\in S_C)} > h\right] \approx Q\left(\frac{h-\mu_1}{\sigma_1}\right)$$

$$\text{and} \quad E[F_{fp}] = P\left[T_N^{(i\notin S_C)} > h\right] \approx Q\left(\frac{h}{\sigma_0}\right). \tag{31}$$

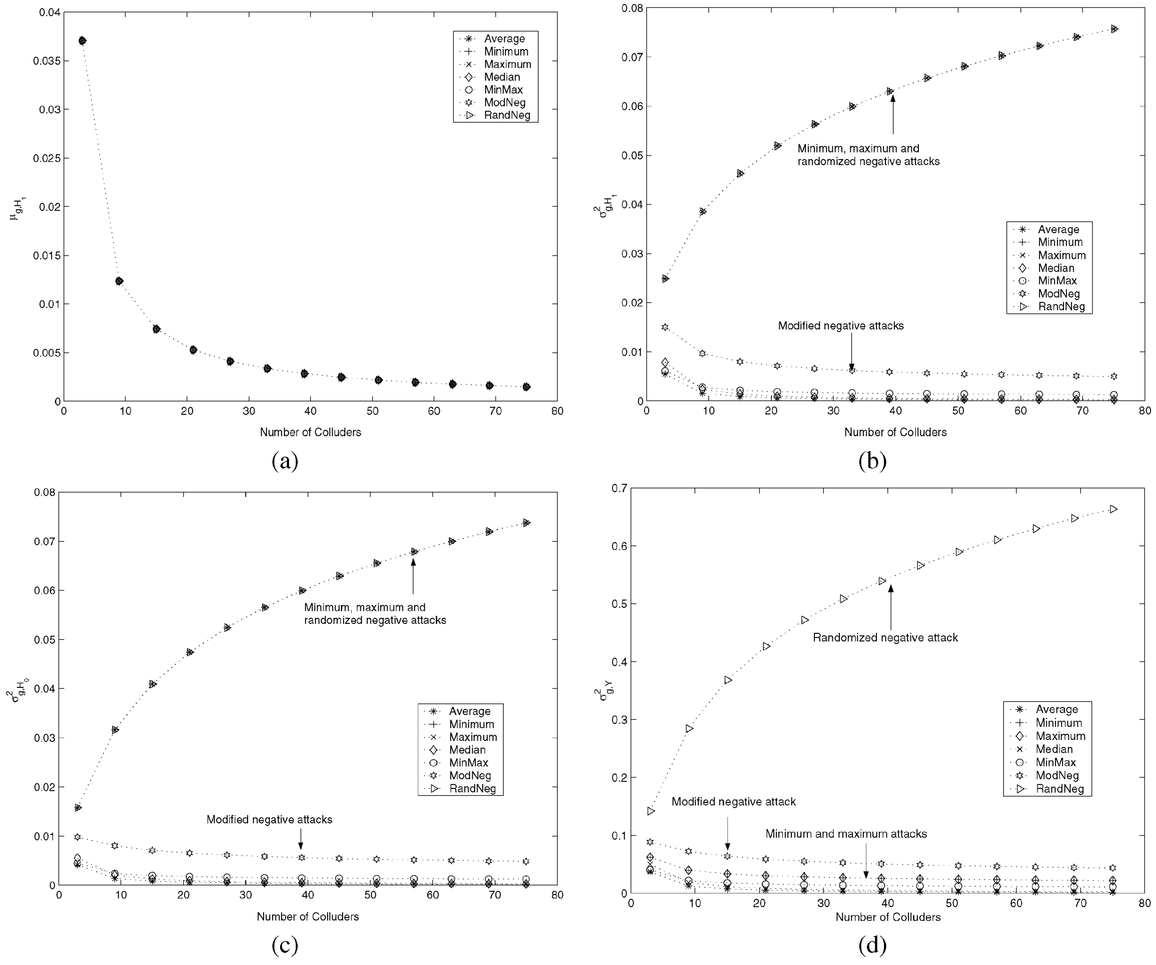
The analysis of P_d, P_{fp}, F_d, and F_{fp} for the Z and q statistics are the same.

2) Perceptual Quality: In our system, the distortion introduced to the host signal by the colluded fingerprint is $n_j = \mathrm{JND}_j \cdot g(\{W_j^{(k)}\}_{k\in S_C})$, $j = 1, 2, \ldots, N$. Given the collusion attack $g(\cdot)$ and the number of colluders K, if $\mathbf{A} \triangleq g(\{W^{(k)}\}_{k\in S_C})$ has the pdf $f_{g,K}(w)$ and $abs(\mathbf{A})$ is the absolute value of $\mathbf{A}$, we can simplify the $\mathrm{MSE}_{\mathrm{JND}}$ and $E[F_{\mathrm{JND}}]$ to

$$\begin{aligned} \mathrm{MSE}_{\mathrm{JND}} &\approx N \times E\left[(abs(\mathbf{A})-1)^2 \mid abs(\mathbf{A}) > 1\right] \\ &= N\int_{-\infty}^{-1}(w+1)^2 f_{g,K}(w)dw \\ &\quad + N\int_1^\infty (w-1)^2 f_{g,K}(w)dw \\ \text{and} \quad E[F_{\mathrm{JND}}] &= P[|\mathbf{A}| > 1] \\ &= \int_{-\infty}^{-1} f_{g,K}(w)dw + \int_1^\infty f_{g,K}(w)dw. \end{aligned} \tag{32}$$

$$f_{W^{\min},W^{\mathrm{med}},W^{(i)}}(W^{\min} = w', W^{\mathrm{med}} = w'', W^{(i)} = w)$$
$$= \begin{cases} 2l\binom{2l-1}{l} f(w')f(w'')[F(w'')-F(w')]^{l-1}[1-F(w'')]^l, & \text{if } W^{\min} = W^{(i)} \\ 2l\binom{2l-1}{l} f(w')f(w'')[F(w'')-F(w')]^{l-1}[1-F(w'')]^l, & \text{if } W^{\mathrm{med}} = W^{(i)} \\ 2l(2l-1)\binom{2l-2}{l-1} f(w')f(w'')f(w)[F(w'')-F(w')]^{l-1}[1-F(w'')]^{l-1}, & \text{if } W^{\mathrm{med}} < W^{(i)} < W^{\max} \\ 2l(2l-1)\binom{2l-2}{l} f(w')f(w'')f(w)[F(w'')-F(w')]^{l-2}[1-F(w'')]^l, & \text{if } W^{\min} < W^{(i)} < W^{\mathrm{med}} \end{cases} \tag{22}$$

$$f_{W^{\mathrm{med}},W^{\max},W^{(i)}}(W^{\mathrm{med}} = w', W^{\max} = w'', W^{(i)} = w)$$
$$= \begin{cases} 2l\binom{2l-1}{l} f(w')f(w'')[F(w'')-F(w')]^{l-1}F^l(w''), & \text{if } W^{\mathrm{med}} = W^{(i)} \\ 2l\binom{2l-1}{l} f(w')f(w'')[F(w'')-F(w')]^{l-1}F^l(w''), & \text{if } W^{\max} = W^{(i)} \\ 2l(2l-1)\binom{2l-2}{l-1} f(w')f(w'')f(w)[F(w'')-F(w')]^{l-1}F^{l-1}(w''), & \text{if } W^{\min} < W^{(i)} < W^{\mathrm{med}} \\ 2l(2l-1)\binom{2l-2}{l} f(w')f(w'')f(w)[F(w'')-F(w')]^{l-2}F^l(w''), & \text{if } W^{\mathrm{med}} < W^{(i)} < W^{\max} \end{cases} \tag{23}$$



(a) (b)

(c) (d)

Fig. 1. (a) μ_{g,H_1}, (b) σ^2_{g,H_1}, (c) σ^2_{g,H_0}, and (d) $\sigma^2_{g,Y}$ of the unbounded Gaussian fingerprints with $\sigma^2_W = 1/9$.

IV. Effectiveness of Collusion Attacks on Gaussian Based Fingerprints

It has been shown in [4] that the uniform fingerprints can be easily defeated by nonlinear collusion attacks, and the simulation results there also showed that the Gaussian fingerprints are more resistant to nonlinear collusion attacks than the uniform fingerprints. However, no analytic study was provided in the literature on the resistance of Gaussian fingerprints to nonlinear collusion attacks. In this section, we study the effectiveness of nonlinear collusion attacks on Gaussian based fingerprints.

A. Unbounded Gaussian Fingerprints

1) Statistical Analysis: We first study the resistance of unbounded Gaussian fingerprints to collusion attacks. As before, we assume that there are a total of M users and the fingerprints $\{W_j^{(i)}\}$ are i.i.d. Gaussian with zero mean and variance σ^2_W. Usually we take $\sigma^2_W \approx 1/9$ to ensure that around 99.9% of fingerprint components are in the range of $[-1, 1]$ and are imperceptible after being scaled by a JND factor.

Under the assumption that the Bernoulli random variable B_p in the randomized negative attack is independent of the zero mean Gaussian fingerprints, we have $E\left[\left(W^{\text{randneg}}\right)^2\right] = E\left[\left(W^{\min}\right)^2\right] = E\left[\left(W^{\max}\right)^2\right]$ for all possible $p \in [0, 1]$. Consequently, we have

$$\begin{aligned}\sigma^2_{\text{randneg},Y} &= E\left[\left(W^{\text{randneg}}\right)^2\right] - \left(E\left[W^{\text{randneg}}\right]\right)^2 \\ &\le E\left[\left(W^{\min}\right)^2\right] \qquad (33)\end{aligned}$$

and the upper bound of the variance in (33) is achieved when $p = 0.5$ and $E\left[W^{\text{randneg}}\right] = 0$. From (30) and (31), the larger the variance, the more effective the attack. Consequently, we take $p = 0.5$ in the randomized negative attack and consider the most effective attack.

Given the analysis in the previous section, we can calculate the parameters μ_{g,H_1}, σ^2_{g,H_1}, σ^2_{g,H_0}, and $\sigma^2_{g,Y}$ for Gaussian distribution with zero mean and variance σ^2_W. Due to the existence of the $Q(\cdot)$ terms in the pdfs and joint pdfs, analytical expressions are not available. We use the recursive adaptive Simpson quadrature method [28] to numerically evaluate the integrals with an absolute error tolerance of 10^{-6} and the results for $\sigma^2_W = 1/9$ are plotted in Fig. 1.

From Fig. 1, we find that, for a given number of colluders K, μ_{g,H_1} are the same for all collusion attacks and equal to σ^2_W/K. Different collusion attacks have different σ^2_{g,H_1}, σ^2_{g,H_0}

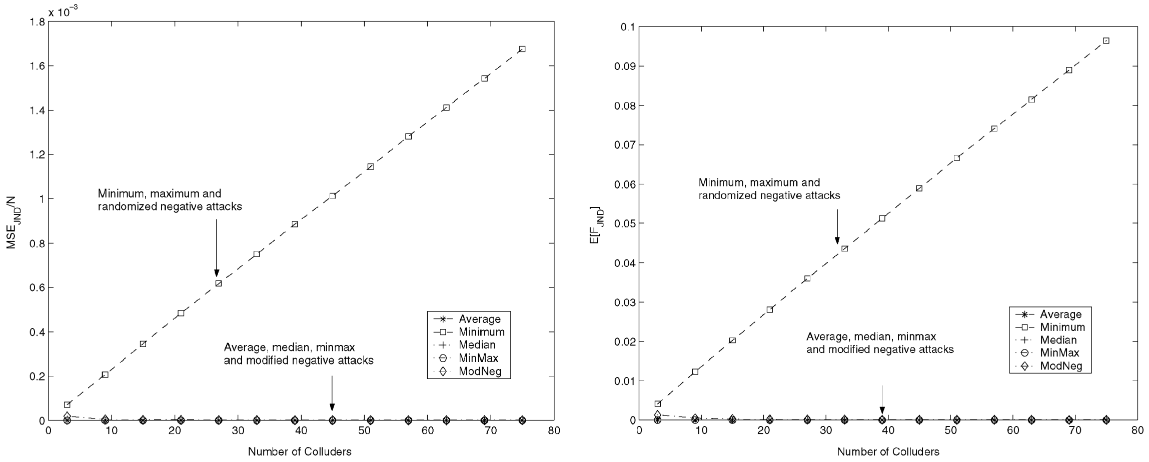


Fig. 2. Perceptual quality of the attacked copy under different attacks with unbounded Gaussian fingerprints. Here, $\sigma_W^2 = 1/9$. (Left) $\mathrm{MSE}_{\mathrm{JND}}/N$. (Right) $E[F_{\mathrm{JND}}]$.

and $\sigma_{g,Y}^2$. The relationship of σ_{g,H_1}^2 and σ_{g,H_0}^2 for different collusion attacks are

$$\begin{aligned}\sigma_{\mathrm{randneg},H_1}^2 &= \sigma_{\mathrm{min},H_1}^2 = \sigma_{\mathrm{max},H_1}^2 > \sigma_{\mathrm{ModNeg},H_1}^2 \\ &> \sigma_{ave,H_1}^2 \approx \sigma_{med,H_1}^2 \approx \sigma_{\mathrm{minmax},H_1}^2 \\ \text{and } \sigma_{\mathrm{randneg},H_0}^2 &= \sigma_{\mathrm{min},H_0}^2 = \sigma_{\mathrm{max},H_0}^2 > \sigma_{\mathrm{ModNeg},H_0}^2 \\ &> \sigma_{ave,H_0}^2 \approx \sigma_{med,H_0}^2 \approx \sigma_{\mathrm{minmax},H_0}^2 \end{aligned} \quad (34)$$

and that of $\sigma_{g,Y}^2$ is

$$\begin{aligned}\sigma_{\mathrm{randneg},Y}^2 &> \sigma_{\mathrm{ModNeg},Y}^2 > \sigma_{\mathrm{min},Y}^2 = \sigma_{\mathrm{max},Y}^2 \\ &> \sigma_{ave,Y}^2 \approx \sigma_{med,Y}^2 \approx \sigma_{\mathrm{minmax},Y}^2. \end{aligned} \quad (35)$$

Note that the extracted fingerprint $\mathbf{Y}$ under the minimum or maximum attack is not zero mean. σ_{g,H_0}^2 is proportional to the second moment of $\mathbf{Y}$, and is the largest under the minimum, maximum, and randomized negative attacks. However, the variance of $\mathbf{Y}$ under the minimum or maximum attacks is small and comparable with $\sigma_{g,Y}^2$ under the average, median, and minmax attacks.

In order to compare the effectiveness of different collusion attacks, we define the following notations.

- Attack A $>$ Attack B: Attack A is more effective than attack B in defeating the system.
- Attack A $=$ Attack B: Attack A and attack B have the same performance in defeating the system.
- Attack A $\approx$ Attack B: Attack A and attack B have similar performance in defeating the system.

From (30), (31), (34), and (35), with the T_N statistics or the q statistics, we can sort different collusion attacks in the descending order of their effectiveness as

$$\begin{aligned}\mathrm{Minimum} &= \mathrm{Maximum} = \mathrm{randneg} > \mathrm{ModNeg} \\ &> \mathrm{Average} \approx \mathrm{Median} \approx \mathrm{MinMax} \end{aligned} \quad (36)$$

and with the Z statistics, we can sort different attacks in the descending order of their effectiveness as

$$\begin{aligned}\mathrm{randneg} &> \mathrm{ModNeg} > \mathrm{Minimum} = \mathrm{Maximum} \\ &> \mathrm{Average} \approx \mathrm{Median} \approx \mathrm{MinMax}. \end{aligned} \quad (37)$$

Therefore, the randomized negative attack is the most effective attack.

So far, we have studied the effectiveness of different collusion attacks. As for the perceptual quality, Fig. 2 shows the $\mathrm{MSE}_{\mathrm{JND}}$ and $E[F_{\mathrm{JND}}]$ of different collusion attacks with i.i.d. $\mathcal{N}(0, 1/9)$ fingerprints. As we can see from Fig. 2, although the minimum, maximum, and randomized negative attacks are more effective in defeating the fingerprinting system, they also introduce larger noticeable distortion that is proportional to the number of colluders.

2) Simulation Results: Our simulation is set up as follows. Since the number of embeddable coefficients in 256×256 and 512×512 images is usually $O(10^4)$, we assume that the length of the fingerprints is 10 000. To accommodate a total of $M = 100$ users, we generate 100 independent fingerprints of length 10 000. Every fingerprint component is independent of each other and follows the $\mathcal{N}(0, 1/9)$ Gaussian distribution. Our results are based on a total of 2000 simulation runs.

In Fig. 3(a) and (c), P_{fp} is fixed as 10^{-2} and we compare P_d of the T_N and Z statistics, respectively, under different collusion attacks. In Fig. 3(b) and (d), $E[F_{fp}]$ is fixed as 10^{-2} and we compare $E[F_d]$ of the T_N and Z statistics, respectively, under different attacks. The performance of the q statistics is similar to that of T_N and is not shown here. We compare different detection statistics with $P_{fp} = 10^{-2}$ in Fig. 3(e) and $E[F_{fp}] = 10^{-2}$ in Fig. 3(f). Note that in Fig. 3(e) and (f), we only plot the performance of the minimum and that of the modified negative attacks since the maximum attack yield the same result as the minimum attack and all other attacks have a similar trend.

The simulation results shown in Fig. 3 agree with our analysis. From Fig. 3(a) and (b), with the T_N or q statistics, the minimum, maximum, and randomized negative attack are the most effective attacks followed by the modified negative attack. The average, median, and minmax attacks are the least effective attacks. From Fig. 3(c) and (d), with the Z statistics, the randomized negative attack is the most effective attack followed by the modified negative attack. The average, median, and minmax attacks have similar performance and they are the least efficient attacks. The minimum and maximum attacks are the second least effective attacks. From Fig. 3(e) and (f), the Z statistics

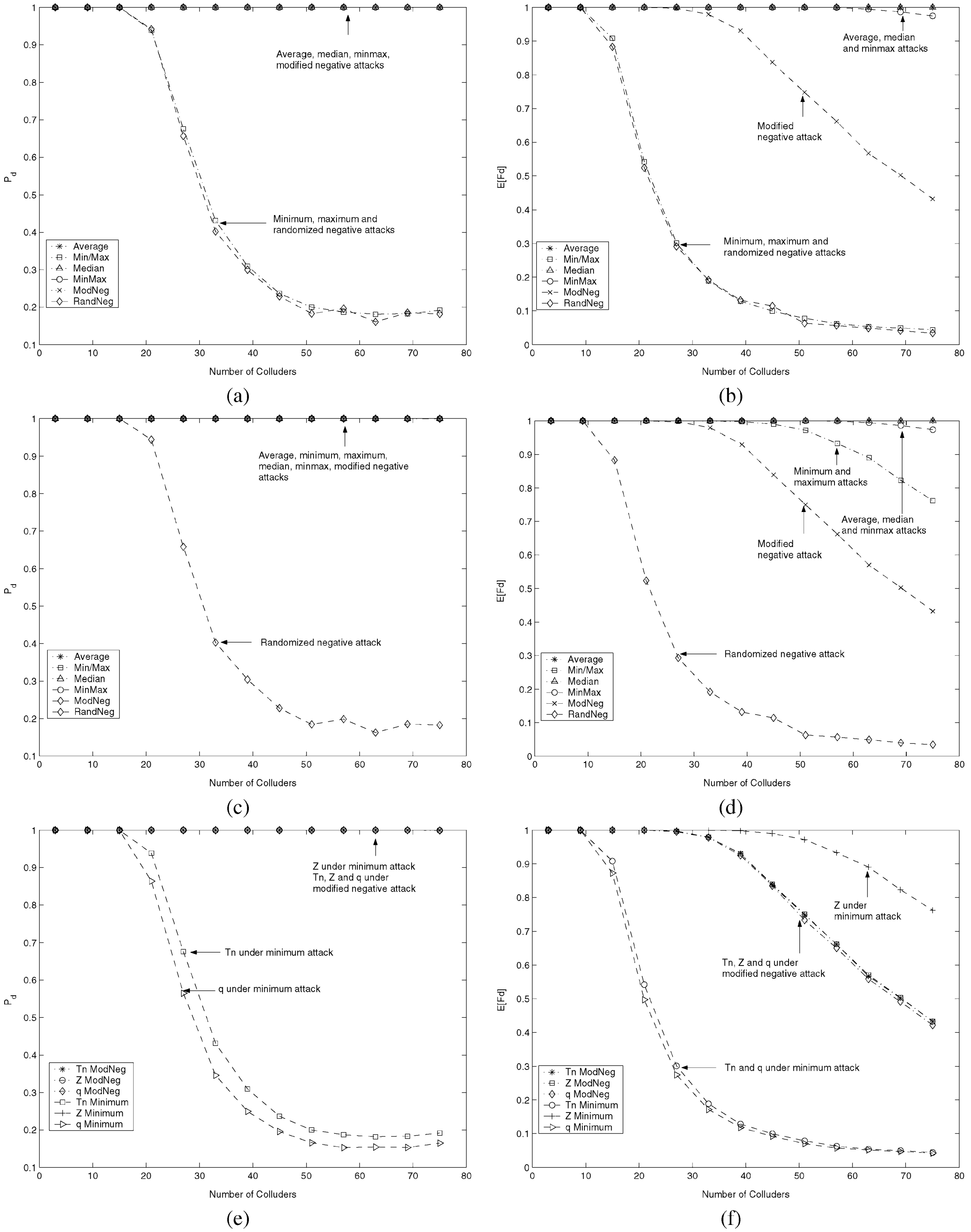


Fig. 3. (a) P_d of the T_N statistics under different attacks, (b) $E[F_d]$ of the T_N statistics under different attacks, (c) P_d of the Z statistics under different attacks, (d) $E[F_d]$ of the Z statistics under different attacks, (e) P_d of different statistics, and (f) $E[F_d]$ of different statistics with unbounded Gaussian fingerprints. Here, $\sigma_W^2 = 1/9$, $M = 100$, and $N = 10^4$. In (a), (c), and (e), $P_{fp} = 10^{-2}$. In (b), (d), and (f), $E[F_{fp}] = 10^{-2}$.

are more resistant to the minimum and maximum attacks than the T_N and q statistics while the three statistics have similar performance under other collusion attacks. Therefore, from the colluders' point view, the best strategy for them is to choose the randomized negative attack. From the detector's point of view, the Z statistics should be used to be more robust against the minimum and maximum attacks.

In Fig. 4, we show the attacked images after the average and the minimum attacks with 75 colluders. Although the minimum, maximum and randomized negative attacks are more effective, they also introduce much larger noticeable distortion in the host image. This is because the fingerprints are not bounded, and in fact, such unbounded fingerprints can introduce noticeable distortion in the fingerprinted copies even when without collusion.

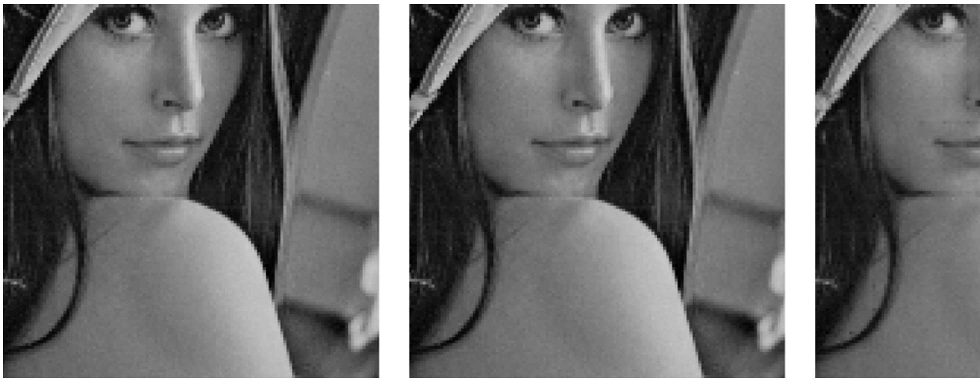


Fig. 4. Comparison of perceptual quality of the attacked images under different attacks with 75 colluders. Fingerprints are generated from unbounded Gaussian distribution with $\sigma_W^2 = 1/9$. (Left) Zoomed-in region of the original 256 × 256 Lena. (Middle) Lena under the average attack. (Right) Lena under the minimum attack.

B. Bounded Gaussian-Like Fingerprints

Compared with uniform fingerprints, Gaussian fingerprints improve the detector's resistance to nonlinear collusion attacks [4] and are resilient to statistical and histogram attacks [20]. Because Gaussian distribution is unbounded, it is possible that the embedded fingerprints exceed the JND and introduce perceptually distinguishable distortion. However, imperceptibility is a requirement of digital fingerprinting and the owner has to guarantee the perceptual quality of the fingerprinted copies. In order to remove the perceptual distortion while maintaining the robustness against collusion attacks, we introduce the bounded Gaussian-like fingerprints and study their performance under collusion attacks.

Assume that $f_X(\cdot)$ and $F_X(\cdot)$ are the pdf and cdf of a Gaussian random variable with zero mean and variance σ_W^2, respectively. The pdf of a bounded Gaussian-like distribution $\tilde{f}_X(\cdot)$ is

$$\tilde{f}_X(x) = \begin{cases} \frac{f_X(x)}{F_X(1)-F_X(-1)}, & \text{if } -1 \le x \le 1 \\ 0, & \text{otherwise.} \end{cases} \quad (38)$$

We can show that the variance of fingerprints following pdf (38) is σ_W^2, and the embedded fingerprints introduce no perceptual distortion since $\mathrm{MSE}_{\mathrm{JND}} = 0$ and $F_{\mathrm{JND}} = 0$. By bounding the fingerprints in the range of $[-1, 1]$, we maintain the energy of the embedded fingerprints while achieving the imperceptibility.

For fingerprints following distribution (38), the analyses of the collusion attacks and the detection statistics are similar to the unbounded case and thus omitted. If we sort different collusion attacks according to their effectiveness, the result is the same as that of the unbounded Gaussian fingerprints.

The simulation of the bounded Gaussian-like fingerprints under collusion attacks is set up similarly to that in Section IV-A.II. Assume that there are a total of $M = 100$ users and the host signal has $N = 10^4$ embeddable coefficients. The i.i.d. fingerprints are generated from the distribution (38) with $\sigma_W^2 = 1/9$. In Fig. 5(a) and (c), $P_{fp} = 10^{-2}$ and we compare P_d of the T_N and Z statistics, respectively, under different collusion attacks. In Fig. 5(b) and (d), $E[F_{fp}] = 10^{-2}$ and we compare $E[F_d]$ of the T_N and Z statistics, respectively, under different collusion attacks. The performance of the q statistics is similar to that of T_N. We compare the performance of different detection statistics under the minimum and the modified negative attacks with $P_{fp} = 10^{-2}$ in Fig. 5(e) and $E[F_{fp}] = 10^{-2}$ in Fig. 5(f), respectively. The simulation results agree with the analysis and we have the same observations as in the unbounded case. From the colluders' point of view, the most efficient attack is the randomized negative attack, and from the detector's point of view, the Z statistics are more robust.

V. Prerocessing of the Extracted Fingerprints

The three detection statistics we have studied so far are not specifically designed for collusion scenarios and, therefore, do not take into account the characteristics of the newly generated copies after the collusion attacks. Intuitively, utilizing the statistical features of the attacked copies may improve the detection performance, and one of such features is the sample mean of the extracted fingerprint under the collusion attacks. From the histogram plots of the extracted fingerprints under different attacks as shown in Fig. 6, we observe different patterns of the sample means of the extracted fingerprints: the extracted fingerprints have approximately zero sample mean under the average, median, minmax and modified negative attacks; the minimum attack yields a negative sample mean, and the maximum attack yields a positive sample mean; and under the randomized negative attack, the histogram of the extracted fingerprint components have two clusters, one with a negative mean and the other with a positive mean.

Recall from Section III-A that σ_{g,H_0}^2 is proportional to the second moment of the extracted fingerprint, subtracting the sample mean from the extracted fingerprint will reduce its second-order moment, thus help improve the detection performance. Similarly, the detection performance under the randomized negative attack can be improved by decreasing σ_{g,H_0}^2 and $\sigma_{g,Y}^2$.

Motivated by this analysis, we propose a preprocessing stage in the detection process: given the extracted fingerprint $\{g(\{W_j^k\}_{k\in S_c})\}_{j=1}^N$, we first investigate its histogram. If a single nonzero sample mean is observed, we subtract

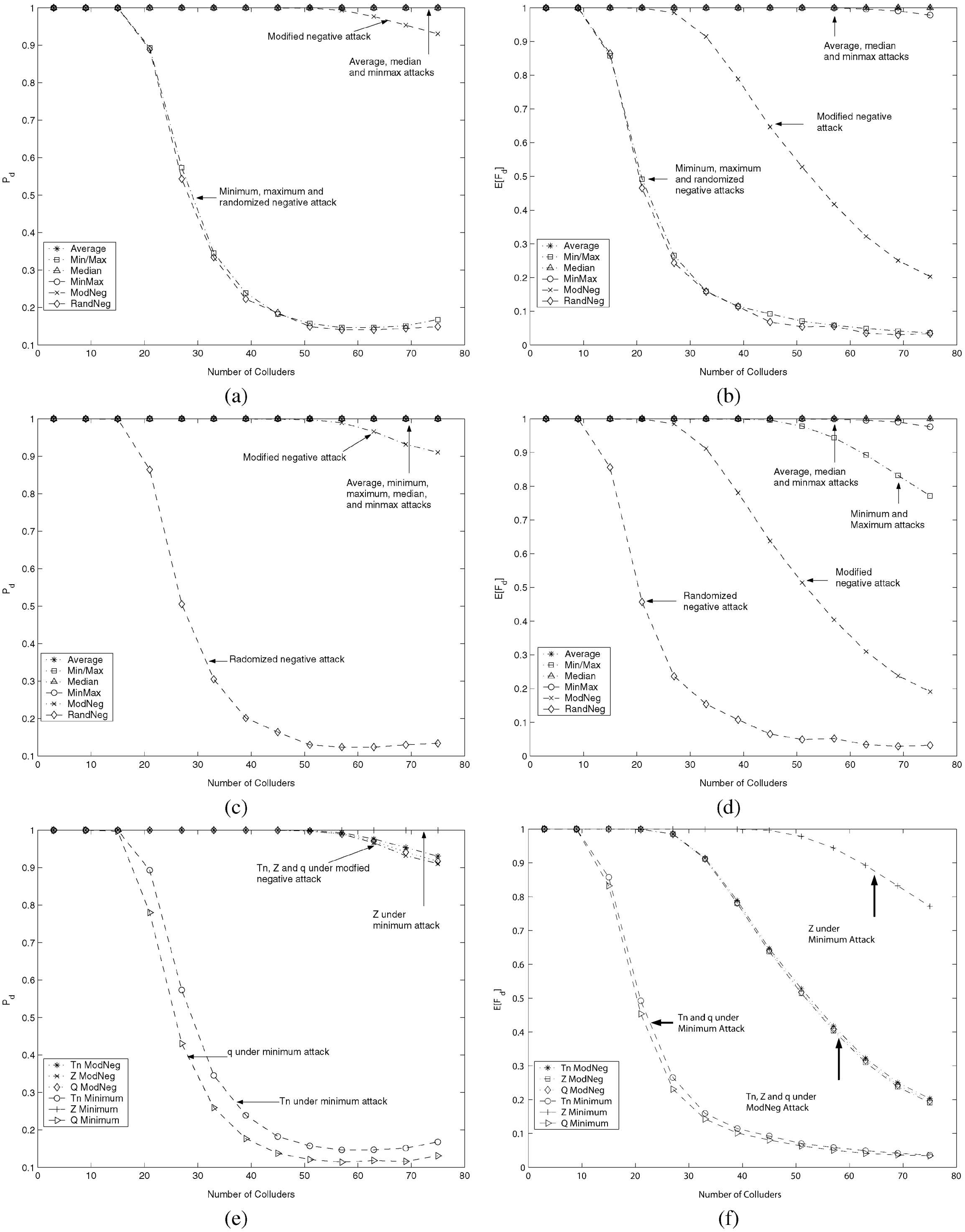


Fig. 5. (a) P_d of the T_N statistics under different attacks, (b) $E[F_d]$ of the T_N statistics under different attacks, (c) P_d of the Z statistics under different attacks, (d) $E[F_d]$ of the Z statistics under different attacks, (e) P_d of different statistics, and (f) $E[F_d]$ of different statistics with bounded Gaussian-like fingerprints. Here, $\sigma_W^2 = 1/9$, $M = 100$, and $N = 10^4$. In (a), (c), and (e), $P_{fp} = 10^{-2}$. In (b), (d), and (f), $E[F_{fp}] = 10^{-2}$.

it from the extracted fingerprint, and then apply the detection statistics. If the fingerprint components are merged from two (or more) distributions that have distinct mean values, we need to cluster components and then subtract from each colluded fingerprint component the sample mean of the corresponding cluster. In the later case, the means can be estimated using a Gaussian-mixture approximation, and the clustering is based on the nearest-neighbor principle. In our problem, under the randomized negative attack, a simple solution is to first observe the bi-modality in the histogram of $\{Y_j\}$, and then cluster all negative components into one distribution and cluster all positive components

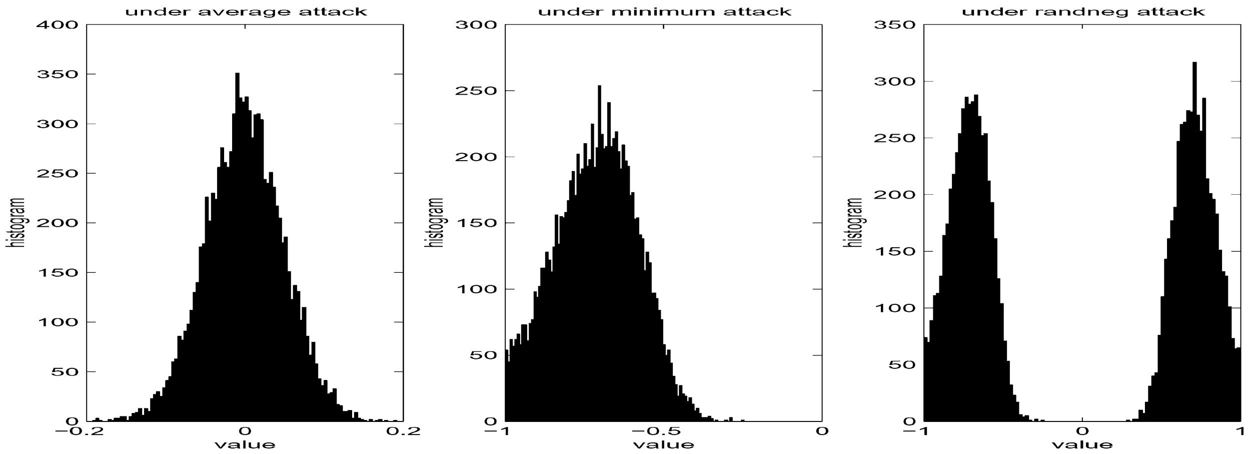
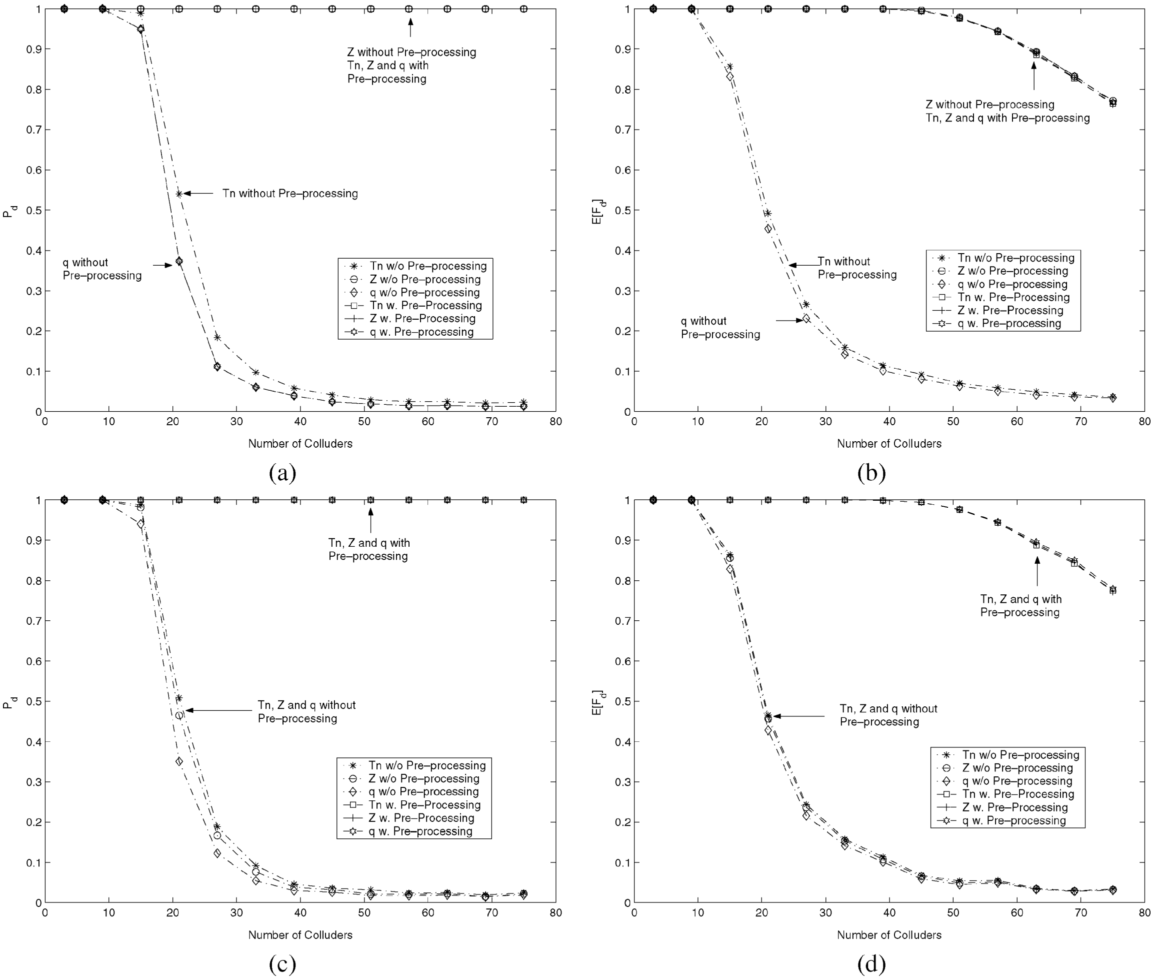


Fig. 6. Histograms of the extracted fingerprints under the average, minimum and randomized negative attacks, respectively. The original fingerprints follow the distribution in (38) with $\sigma_W^2 = 1/9$. $N = 10^4$ and $K = 45$.



(a)

(b)

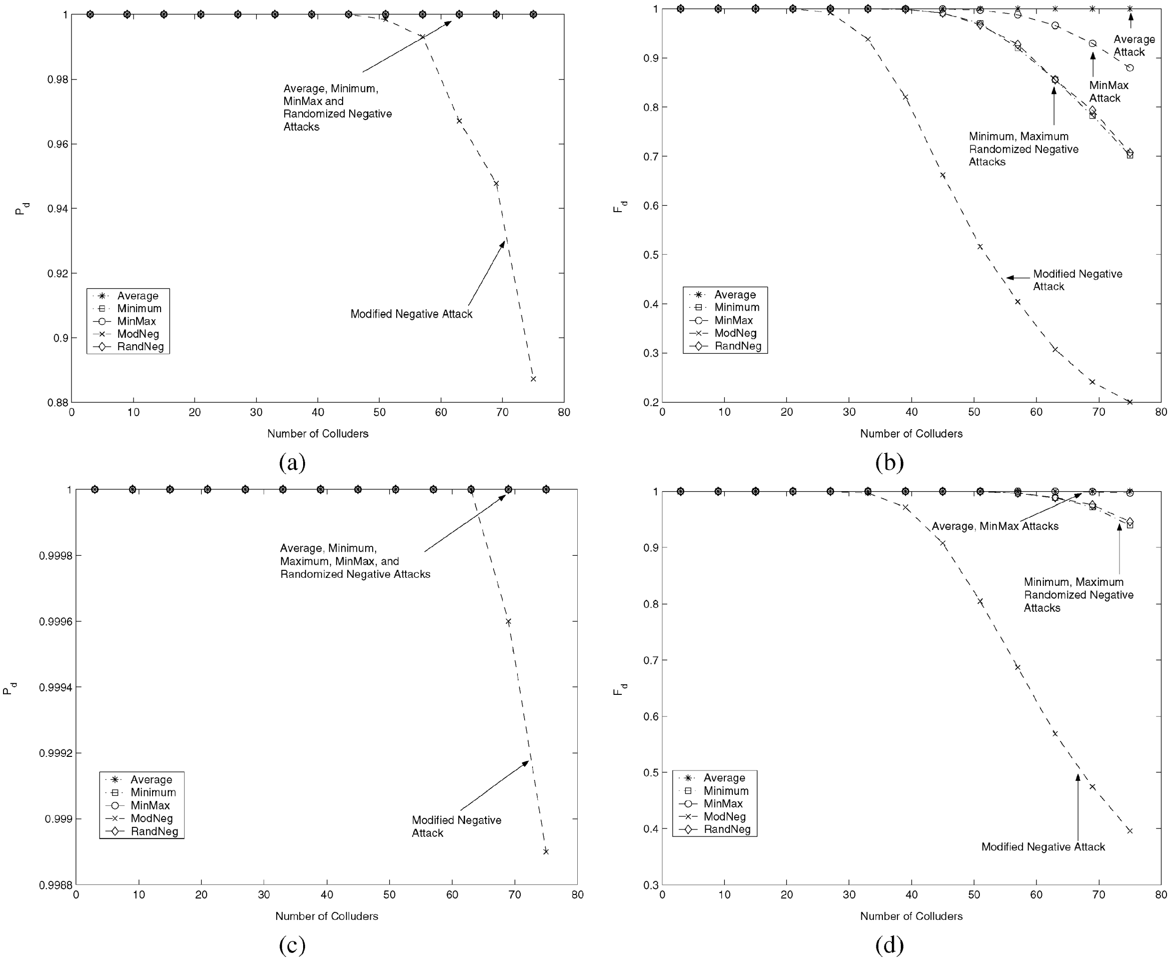
(c)

(d)

Fig. 7. (a) P_d under the minimum attack, (b) $E[F_d]$ under the minimum attack, (c) P_d under the randomized negative attack, and (d) $E[F_d]$ under the randomized negative attack with and without preprocessing. Fingerprints are generated from bounded Gaussian-like distribution (38) with $\sigma_W^2 = 1/9$. $M = 100$ and $N = 10^4$. In (a) and (c), $P_{fp} = 10^{-2}$. In (b) and (d), $E[F_{fp}] = 10^{-2}$.

into the other distribution. Given the extracted fingerprint $\{Y_j\}_{j=1}^N$, define $\mu_{\text{neg}} \triangleq \sum_j Y_j \cdot I[Y_l < 0] / \sum_l I[Y_l < 0]$ as the sample mean of the negative components of the extracted fingerprint where $I[\cdot]$ is the indication function, and $\mu_{\text{pos}} \triangleq \sum_j Y_j \cdot I[Y_j > 0] / \sum_l I[Y_l > 0]$ as the sample mean of the positive components of the extracted fingerprint. Then the preprocessing stage generates

$$Y_j' = \begin{cases} Y_j - \mu_{\text{neg}}, & \text{if } Y_j < 0 \\ Y_j - \mu_{\text{pos}}, & \text{if } Y_j > 0 \end{cases} \tag{39}$$



(a) (b) (c) (d)

Fig. 8. (a) P_d of Lena, (b) $E[F_d]$ of Lena, (c) P_d of Baboon, and (d) $E[F_d]$ of Baboon with the Z statistics under different collusion attacks. The original fingerprints follow the distribution in (38) with $\sigma_W^2 = 1/9$. $M = 100$. In (a) and (b), the length of the embedded fingerprints is $N = 13\,691$. In (c) and (d), the length of the embedded fingerprints is $N = 19\,497$. In (a) and (c), $P_{fp} = 10^{-2}$ and simulation results are based on 10,000 simulation runs. In (b) and (d), $E[F_{fp}] = 10^{-2}$ and simulation results are based on 1,000 simulation runs.

and the detector applies the detection statistics to $\{Y_j'\}_{j=1}^N$. The analysis of the detection statistics with the preprocessing is the same as in Section III and is not repeated.

The simulation is set up the same as before and the fingerprint components are generated from the bounded Gaussian-like distribution (38) with $\sigma_W^2 = 1/9$. In Fig. 7(a) and (c), with $P_{fp} = 10^{-2}$, we compare P_d of the three statistics with and without the preprocessing under the minimum and the randomized negative attacks, respectively. In Fig. 7(b) and (d), with $E[F_{fp}] = 10^{-2}$, we compare $E[F_d]$ of the three statistics with and without the preprocessing under the minimum and the randomized negative attacks, respectively. The detection performance under the maximum attack is the same as that of the minimum attack and is not shown here. We can see that the preprocessing substantially improves the detection performance of the detector, and the three statistics have similar performance under the minimum, maximum, and randomized negative attacks.

Note that the estimated correlation coefficient $\rho^{(i)}$ in the Z statistics removes the mean of the extracted fingerprint before calculating the correlation between the extracted fingerprint and the original fingerprint. This explains why the Z statistics perform better than the T_N and q statistics without preprocessing under the minimum and maximum attacks, whereby the mean of the colluded fingerprint components is substantially deviated from zero.

VI. Simulation Results on Real Images

To study the performance of Gaussian based fingerprints under different nonlinear collusion attacks on real images, we choose two 256×256 host images, Lena and Baboon, which have a variety of representative visual features such as the texture, sharp edges, and smooth areas. We use the human visual model based spread spectrum embedding in [23], and embed the fingerprints in the DCT domain. The generated fingerprints follow the bounded Gaussian-like distribution (38) with $\sigma_W^2 = 1/9$. 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. Then the detector applies the preprocessing to the extracted fingerprint if a nonzero sample mean is observed. Finally, the detector uses the detection statistics to identify the colluders.

Fig. 8 shows the simulation results of the Z statistics. The T_N and q statistics have similar performance and are not shown here. We assume that there are a total of $M = 100$ users. In Fig. 8(a) and (c), we fix $P_{fp} = 10^{-2}$ and compare P_d of Lena and Baboon, respectively, under different nonlinear collusion attacks. In Fig. 8(b) and (d), we fix $E[F_{fp}] = 10^{-2}$ and compare $E[F_d]$ of Lena and Baboon, respectively, under different nonlinear collusion attacks. The simulation results from real images agree with our analysis in Section III, and are comparable to the simulation results in Sections IV and V. In addition, a better performance is observed in the Baboon example than in Lena. This is because the length of the embedded fingerprints in Baboon, which is $N = 19\,497$, is larger than that in Lena, which is $N = 13\,691$. Different characteristics of the two images, e.g., smooth regions and the texture, also contribute to the difference in performance.

VII. A Few More Collusion Attacks

Besides of the attacks listed in (1), we further consider a few other possible collusion attacks. One of them is the *copy and paste attack* where in generating each component of the attacked copy V_j, the colluders equiprobably choose one of the K different copies $\{X_j^{(k)}\}_{k \in S_C}$ and take that value as V_j. In terms of the effects on the energy reduction of the original fingerprints and the effect it has upon the detection performance, this attack and the average attack have similar performance.

Another possible attack is on bounded fingerprints. Since all the K embedded fingerprints are within the range of $[-\mathrm{JND}, \mathrm{JND}]$, so are the minimum and the maximum of these K copies. The minimum and the maximum values also tell the colluders the lower and upper bounds of the possible fingerprints that will not introduce noticeable distortion. The colluders can randomly choose any value between the minimum and the maximum as the colluded copy without introducing perceptual distortion. We call it the *uniform attack*, which can be modeled as the minmax attack followed by an additive noise $\mathbf{n}$. The extracted fingerprint is $\{Y_j = (1/2)(W_j^{\min} + W_j^{\max}) + n_j\}_{j=1}^N$ where n_j is uniformly distributed in $[-(W_j^{\max} - W_j^{\min})/2, (W_j^{\max} - W_j^{\min})/2]$. When K is large, $\{n_j\}$ are approximately uniformly distributed in $[-1, 1]$. Note that in addition to the collusion functions listed in (1), the colluders can also add another additive noise to the attacked copy, as long as the overall distortion introduced in the host signal (the extracted fingerprint plus the additive noise in this case) is bounded by JND. This additional noise will hinder the detection performance without degrading the perceptual quality of the attacked signal. We can show that given a fixed power of the overall noise introduced in the host signal, different collusion attacks have comparable performance in defeating the fingerprinting systems.

VIII. Conclusion

In this paper, we have provided theoretical analysis on the effectiveness of different collusion attacks and studied the perceptual quality of the attacked signals under different collusion attacks. We have also studied several commonly used detection statistics and compared their performance under collusion attacks. Furthermore, we have proposed the preprocessing techniques specifically for collusion scenarios to improve the detection performance.

We first studied the effectiveness of average and various basic nonlinear collusion attacks with unbounded Gaussian fingerprints. From both our analytical and simulation results, we found that with the three detection statistics as defined in the literature and without any modification, the randomized negative attack is the most effective attack against the fingerprinting system. We showed that the Z statistics are more robust against the minimum and maximum attacks than the other two statistics by implicitly removing the mean of the extracted fingerprint. We also showed that all three statistics have similar performance under other collusion attacks. However, the unbounded Gaussian fingerprints may exceed JND and introduce perceptual distortion in the host signal even when without collusion, and the minimum, maximum, and randomized negative attacks introduce much larger distortion in the attacked copies than others.

In order to remove the noticeable distortion introduced by the unbounded fingerprints, we proposed the bounded Gaussian-like fingerprints, which maintain the robustness against the collusion attacks. With the bounded Gaussian-like fingerprints, the randomized negative attack is still the most effective attack, and the Z statistic are more robust against the minimum and maximum attacks than the other two statistics. The bounding improves the perceptual quality of the fingerprinted copies and that of the attacked copies, and both the fingerprint designer and the colluders do not introduce noticeable distortion.

Observing that the extracted fingerprints under the minimum and the maximum attacks do not have a zero mean, we proposed the preprocessing of the extracted fingerprints, which removes the mean from the extracted fingerprints before applying the detection statistics. We also applied preprocessing to the extracted fingerprints after the randomized negative attacks, which have distinct bimodal distribution as opposed to the single modality under other collusions. We showed that these preprocessing techniques improve the detection performance, and all detection statistics give similar performance after preprocessing.

We have also studied the effectiveness of different collusion attacks and the performance of different statistics on real images. Our real image simulation results agree with our analysis and are comparable with the ideal case simulation results.

Acknowledgment

The authors would like to thank Dr. W. Trappe at WINLAB, ECE Department, Rutgers University, for his constructive suggestions and inspiring discussions.

References

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

[2] F. Petitcolas, R. Anderson, and M. Kuhn, "Information hiding – A survey," *Proc. IEEE*, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[3] G. C. Langelaar, I. Setyawan, and R. Lagendijk, "Watermarking digital image and video data: A state-of-the-art overview," *IEEE Signal Process. Mag.*, vol. 17, no. 9, pp. 20–46, Sep. 2000.

[4] H. Stone, "Analysis of Attacks on image watermarks with randomized coefficients," NEC Res. Inst., Tech. Rep. 96–045, 1996.

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

[6] F. Petitcolas, R. Anderson, and M. Kuhn, "Attacks on copyright marking systems," in *Proc. 2nd Workshop Information Hiding*, Apr. 1998, pp. 218–238.

[7] I. Cox and J. Linnartz, "Some general methods for tampering with watermaking," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 5, pp. 587–593, May 1998.

[8] F. Hartung, J. Su, and B. Girod, "Spread spectrum watermarking: Malicious attacks and counterattacks," *Proc. SPIE*, pp. 147–158, Jan. 1999.

[9] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inf. Theory*, vol. 44, no. 5, pp. 1897–1905, Sep. 1998.

[10] B. Chor, A. Fiat, and M. Manor, "Tracing traitors," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 893–910, May 2000.

[11] Y. Yacobi, "Improved Boneh-Shaw content fingerprinting," in *Proc. The Cryptographer's Track at RSA Conf.*, vol. 2020, 2001, pp. 378–391.

[12] A. Fiat and T. Tassa, "Dynamic tracing traitors," in *Proc. Advances*, vol. 1666, 1999, pp. 354–371.

[13] B. Pfitzmann and M. Waidner, "Asymmetric fingerprinting for larger collusions," in *Proc. 4th ACM Conf. Computer and Communication Security*, 1997, pp. 151–160.

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

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

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

[17] F. Ergun, J. Killian, and R. Kumar, "A note on the limits of collusion-resistant watermarks," in *Proc. Advances in Cryptology*, vol. 1592, 2001, pp. 140–149.

[18] J. Killian, T. Leighton, L. R. Matheson, T. G. Shamoon, R. Tajan, and F. Zane, "Resistance of digital watermarks to collusive attacks," Dep. Comp Sci., Princeton Univ., Tech. Rep. TR-585–98, 1998.

[19] J. Su, J. Eggers, and B. Girod, "Capacity of digital watermarks subject to an optimal collusion attacks," presented at the Eur. Signal Processing Conf., 2000.

[20] S. Craver, B. Liu, and W. Wolf, "Histo-cepstral analysis for reverse-engineering watermarks," in *Proc. 38th Conf. Information Sciences and Systems*, Mar. 2004, pp. 824–826.

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

[22] W. Zeng and B. Liu, "A statistical watermark detection technique without using original images for resolving right ownerships of digital images," *IEEE Trans. Image Process.*, vol. 8, no. 11, pp. 1534–1548, Nov. 1999.

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

[24] C. Lin, M. Wu, J. Bloom, M. Miller, I. Cox, and Y. Liu, "Rotation, scale, and translation resilient public watermarking for images," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 767–782, May 2001.

[25] J. Lubin, J. Bloom, and H. Cheng, "Robust, content-dependent, high-fidelity watermark for tracking in digital cinema," *Proc. SPIE*, vol. 5020, pp. 536–545, Jun. 2003.

[26] Z. J. Wang, M. Wu, H. Zhao, W. Trappe, and K. J. R. Liu, "Resistance of orthogonal Gaussian fingerprints to collusion attacks," in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing*, vol. IV, Apr. 2003, pp. 724–727.

[27] H. A. David, *Order Statistics*, 2nd ed. New York: Wiley, 1981.

[28] W. Gander and W. Gautschi, "Adaptive quadrature – Revised," *BIT*, vol. 40, no. 1, pp. 84–101, Mar. 2000.

[29] M. Wu, W. Trappe, Z. J. Wang, K. J. R. Liu, and W. Gautschi, "Collusion resistant fingerprint for multimedia," *IEEE Signal Process. Mag.*, no. 3, pp. 15–27, Mar. 2004.

[30] H. Zhao, M. Wu, Z. J. Wang, and K. J. R. Liu, "Nonlinear collusion attacks on digital fingerprinting," in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing*, vol. 5, Apr. 2003, pp. 664–667.

[31] H. Zhao, M. Wu, Z. J. Wang, and K. J. R. Liu, "Performance of detection statistics under collusion attacks on independent multimedia fingerprints," in *Proc. IEEE Int. Conf. Multimedia*, vol. 1, Jul. 2003, pp. 205–208.

[32] Z. J. Wang, M. Wu, W. Trappe, and K. J. R. Liu, "Anti-collusion of group-oriented fingerprinting," in *Proc. IEEE Int. Conf. Multimedia*, vol. 1, Jul. 2003, pp. 217–220.

[33] Z. J. Wang, M. Wu, W. Trappe, and K. J. R. Liu, "Group-oriented fingerprinting for multimedia forensics," *EURASIP J. Appl. Signal Process.*, pp. 2142–2162, Nov. 2004.

H. Vicky Zhao (S'02–M'05) received the B.S. and M.S. degrees from Tsinghua University, Beijing, China, in 1997 and 1999, respectively, and the Ph.D. degree from the University of Maryland, College Park, in 2004, all in electrical engineering.

Since 2005, she has been a Research Associate with the Department of Electrical and Computer Engineering and Institute for Systems Research, University of Maryland. Her research interests include multimedia security, digital rights management, multimedia communication over networks, and multimedia signal processing.

Min Wu (S'95–M'01) received the B.Eng. degree in electrical engineering and the B.A. degree in economics (both with the highest honors) from Tsinghua University, Beijing, China, in 1996 and the M.A. degree and Ph.D. degree in electrical engineering from Princeton University, Princeton, NJ, in 1998 and 2001, respectively.

She was with NEC Research Institute, Princeton, NJ, in 1998 and Panasonic Information and Networking Laboratories, Princeton, in 1999. Since 2001, she has been an Assistant Professor with the Department of Electrical and Computer Engineering, Institute of Advanced Computer Studies and the Institute of Systems Research, University of Maryland, College Park. She is a Guest Editor of the Special Issue on Media Security and Rights Management for the *EURASIP Journal on Applied Signal Processing*. She co-authored the book *Multimedia Data Hiding* (New York: Springer-Verlag, 2003) and holds four U.S. patents on multimedia security. Her research interests include information security, multimedia signal processing, and multimedia communications.

Dr. Wu received a CAREER award from the U.S. National Science Foundation in 2002, a George Corcoran Faculty Award from University of Maryland in 2003, a TR100 Young Innovator Award from MIT Technology Review Magazine in 2004, and a Young Investigator Award from U.S. Office of Naval Research in 2005. She is a member of the IEEE Technical Committee on Multimedia Signal Processing and was the Publicity Chair of the 2003 IEEE International Conference on Multimedia and Expo.

Z. Jane Wang (M'02) received the B.Sc. degree (with the highest honors) from Tsinghua University, Beijing, China, in 1996 and the M.Sc. and Ph.D. degrees from the University of Connecticut, Storrs, in 2000 and 2002, respectively, all in electrical engineering.

She has been a Research Associate with the Electrical and Computer Engineering Department, Institute for Systems Research at the University of Maryland, College Park. Since August 2004, she has been an Assistant Professor with the Department Electrical and Computer Engineering, University of British Columbia, Vancouver, BC, Canada. Her research interests are in the broad areas of statistical signal processing, with applications to information security, biomedical imaging, genomic, and wireless communications.

Dr. Wang received the Outstanding Engineering Doctoral Student Award while at the University of Connecticut.

K. J. Ray Liu (F'03) received the B.S. degree from the National Taiwan University, Taiwan, R.O.C., in 1983 and the Ph.D. degree from the University of California, Los Angeles, in 1990, both in electrical engineering.

He is a Professor and Director of Communications and Signal Processing Laboratories of Electrical and Computer Engineering Department and Institute for Systems Research, University of Maryland, College Park. He was the founding Editor-in-Chief of the *EURASIP Journal on Applied Signal Processing*. His research contributions encompass broad aspects of information forensics and security; wireless communications and networking; multimedia communications and signal processing; signal processing algorithms and architectures; and bioinformatics, in which he has published over 350 refereed papers.

Dr. Liu is the recipient of numerous honors and awards, including the IEEE Signal Processing Society's 2004 Distinguished Lecturer; the 1994 National Science Foundation's Young Investigator Award; the IEEE Signal Processing Society's 1993 Senior Award (Best Paper Award); the IEEE 50th Vehicular Technology Conference Best Paper Award, Amsterdam, The Netherlands, 1999; and the EURASIP 2004 Meritorious Service Award. He also received the George Corcoran Award in 1994 for outstanding contributions to electrical engineering education and the Outstanding Systems Engineering Faculty Award in 1996 in recognition for outstanding contributions in interdisciplinary research, both from the University of Maryland. He is the Editor-in-Chief of *IEEE Signal Processing Magazine*, the prime proposer and architect of the new IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and was the founding Editor-in-Chief of *EURASIP Journal on Applied Signal Processing*. He is a member of Board of Governors of IEEE Signal Processing Society.