PERFORMANCE OF DETECTION STATISTICS UNDER COLLUSION ATTACKS ON INDEPENDENT MULTIMEDIA FINGERPRINTS

Hong Zhao, Min Wu, Z. Jane Wang, and K. J. Ray Liu

Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742

ABSTRACT

Digital fingerprinting is a technology for tracing the distribution of multimedia content and protecting them from unauthorized redistribution. Collusion attack is a cost effective attack against digital fingerprinting where several copies with the same content but different fingerprints are combined to remove the original fingerprints. In this paper, we consider average attack and several nonlinear collusion attacks on independent Gaussian based fingerprints, and study the detection performance of several commonly used detection statistics in the literature under collusion attacks. Observing that these detection statistics are not specifically designed for collusion scenarios and do not take into account the characteristics of the newly generated fingerprints under collusion attacks, we propose pre-processing techniques to improve the detection performance of the detection statistics under collusion attacks.

1. INTRODUCTION

With the rapid development of multimedia and communication technologies, an increasing amount of multimedia data are distributed through networks. This introduces an urgent demand to insure the proper distribution and usage of content, especially considering the ease of manipulating digital multimedia data.

To prevent illegal redistribution of the multimedia content, a digital fingerprinting system embeds unique identification information into each distributed copy to trace customers who use their copies inappropriately. There is a cost effective attack against digital fingerprinting, known as *collusion*. In collusion attacks, several users (colluders) get together, combine information from different fingerprinted copies of the same host signal and generate a new copy where the original fingerprints are removed or attenuated [1]. Digital fingerprinting should be resistant to collusion attacks as well as to common signal processings.

In the literature, there are several commonly used detection statistics [1, 2, 3] available for the detection of the existence of the additively embedded watermark in the test signals. To our knowledge, there is no work that compares their detection performance under collusion attacks. Also, these detection statistics are not specifically designed for detection of fingerprints under collusion attacks and ignore the statistical characteristics of the colluded fingerprints under different collusion attacks. In this paper, we focus on average and several nonlinear collusion attacks [1] on independent Gaussian based fingerprints and study the detection performance of different statistics under collusion attacks. We also take into consideration the statistical features of the colluded fingerprints in the detection process to improve the detection performance under collusion attacks.

The paper is organized as follows. Section 2 introduces the fingerprinting and collusion attack system model. In Section 3, we analyze the detection performance of the detection statistics under collusion attacks. In Section 4, we study the performance of the statistics on independent Gaussian based fingerprints. Section 5 proposes the pre-processing stage to improve the detection performance of the statistics. Conclusions are drawn in Section 6.

2. SYSTEM MODEL

We consider a system that consists of three parts: fingerprint embedding, collusion attacks, and fingerprint detection. Spread spectrum watermark embedding [4, 5] is widely used in watermark applications where the robustness of the watermark is required. Assume that there are a total of M users in the system. Given a host signal represented by a vector $\mathbf{S}$ with length N, the owner chooses a unique fingerprint $\mathbf{W}^{(i)}$ of length N for user $i = 1, \cdots, M$, and generates the fingerprinted copy $\mathbf{X}^{(i)}$ by $\mathbf{X}^{(i)} = \mathbf{S} + \alpha \mathbf{W}^{(i)}$. α is the *Just-Noticeable-Difference (JND)* from human visual models [5] to control the energy and guarantee the imperceptibility of the embedded fingerprints. We assume that the M fingerprints $\{\mathbf{W}^{(i)}\}$ are chosen independently.

Assume that K users collude and S_C 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 ($j = 1, \cdots, N$) component of the attacked copy $\mathbf{V} = [V_1, V_2, \cdots, V_N]^T$ using one of the following collusion functions:

$$\begin{array}{lll} \text{average:} & V_j^{ave} & = \sum_{k \in S_C} X_j^{(k)} / K, \\ \text{minimum:} & V_j^{min} & = \min_{k \in S_C} \{X_j^{(k)}\}, \\ \text{maximum:} & V_j^{max} & = \max_{k \in S_C} \{X_j^{(k)}\}, \\ \text{randomized negative:} & V_j^{randneg} & = \begin{cases} V_j^{min} & \text{with prob. } p, \\ V_j^{max} & \text{with prob. } 1-p. \end{cases} \end{array} \qquad (1)$$

In this paper, we assume that p in the randomized negative attack is independent of the fingerprints $\{W_j^{(i)}\}$ and $p = 0.5$. Analyses of other nonlinear collusion attacks are available in [6]. Note that for our model, applying the collusion attacks to the fingerprinted copies is equivalent to applying the collusion attacks to the fingerprints. For example, $\mathbf{V}^{min} = \min_{k \in S_C} \{\mathbf{S} + \alpha \mathbf{W}^{(k)}\} = \mathbf{S} + \alpha \min_{k \in S_C} \{\mathbf{W}^{(k)}\}$.

The authors can be reached at hzhao, minwu, wangzhen and kjrliu@eng.umd.edu

0-7803-7965-9/03/$17.00 ©2003 IEEE

In the detection process, the detector removes the host signal from $\mathbf{V}$ and extracts the fingerprint $\mathbf{Y} = g(\{\mathbf{W}^{(k)}\}_{k \in S_C})$, where $g(\cdot)$ is the collusion function defined in (1). The detector measures the similarity between $\mathbf{Y}$ and each of the M original fingerprints $\{\mathbf{W}^{(i)}\}$, compares with a threshold, and outputs the estimated colluder set. In the literature, three detection statistics [1, 2, 3] are used to measure the similarity between the extracted fingerprint and the original fingerprint [1]:

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

In (2), $\|\mathbf{W}^{(i)}\|$ is the Euclidean norm of $\mathbf{W}^{(i)}$, N is the length of the watermark, ρ is the estimated correlation coefficient between $\mathbf{Y}$ and $\mathbf{W}^{(i)}$, $\hat{\sigma}_W^2 = \frac{1}{N-1}\sum_j (W_j^{(i)} - \frac{1}{N}\sum_{j=1}^{N} W_j^{(i)})^2$ and $\hat{\sigma}_Y^2 = \frac{1}{N-1}\sum_j (Y_j - \frac{1}{N}\sum_{j=1}^{N} Y_j)^2$ 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 $\{Y_j W_j^{(i)}\}$.

We adopt the commonly used criteria to measure the detection performance of the three statistics under collusion attacks: the probability of capturing at least one colluder (P_d) and the probability of accusing at least one innocent user (P_{fp}). We also considered other measurements like the fraction of colluders that are successfully captured and the fraction of users that are innocently accused. From the analysis in [6], they have the same tendency as P_d and P_{fp}, and therefore are not included in this paper.

3. ANALYSIS OF THE DETECTION STATISTICS UNDER COLLUSION ATTACKS

3.1. Analysis of the Correlation Term

Note that, in (2), all detection statistics are correlation based, and the kernel term is the linear correlation between the extracted fingerprint $\mathbf{Y}$ and the original fingerprint $\mathbf{W}^{(i)}$

$$
T_N^{'(i)} \triangleq \frac{1}{N} < \mathbf{Y}, \mathbf{W}^{(i)} >= \frac{1}{N}\sum_{j=1}^{N} g(\{W_j^{(k)}\}_{k \in S_c}) W_j^{(i)} \qquad (3)
$$

where N is the length of the fingerprint and $T_N^{'(i)}$ can be regarded as the unnormalized T_N statistics for user i.

Under the assumption that $\{W_j^{(k)}\}$ 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 they have finite mean μ and finite variance σ^2, then we can approximate $T_N^{'(i)}$ with the following Gaussian distribution:

$$
T_N^{'(i)} \sim \mathcal{N}\left(\mu, \sigma^2/N\right). \qquad (4)
$$

Therefore, we need to find $\mu = E[g(\{W^{(k)}\}_{k \in S_c}) W^{(i)}]$ and $\sigma^2 = var[g(\{W^{(k)}\}_{k \in S_c}) W^{(i)}]$ (for simplicity, we will drop the subscript j). Due to the symmetry of $g(\{W^{(k)}\}_{k \in S_c}) W^{(i)}$ with respect to the user i, with the same collusion function and the same number of colluders, all $g(\{W^{(k)}\}_{k \in S_c}) W^{(i)}$ where $i \in S_C$ have the same mean and variance. 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

$$
\begin{aligned}
\mu_{g,H_1} &\triangleq E\left[g(\{W^{(k)}\}_{k \in S_c}) W^{(i)}\right], \qquad (5)\\
\text{and} \quad \sigma_{g,H_1}^2 &\triangleq var\left[g(\{W^{(k)}\}_{k \in S_c}) W^{(i)}\right].
\end{aligned}
$$

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

$$
\begin{aligned}
\mu_{g,H_0} &\triangleq E\left[g(\{W^{(k)}\}_{k \in S_c}) W^{(i)}\right] = 0,\\
\text{and} \quad \sigma_{g,H_0}^2 &\triangleq var\left[g(\{W^{(k)}\}_{k \in S_c}) W^{(i)}\right]\\
&= E\left[g^2(\{W^{(k)}\}_{k \in S_c})\right] \sigma_W^2. \qquad (6)
\end{aligned}
$$

Detailed derivation of μ_{g,H_1}, σ_{g,H_1}^2 and σ_{g,H_0}^2 under different collusion attacks is available in [6].

From (4), (5) and (6), $T_N^{'(i)}$ can be approximated with the following Gaussian distribution

$$
T_N^{'(i)} \sim \begin{cases} \mathcal{N}\left(0, \frac{\sigma_{g,H_0}^2}{N}\right) & \text{if } i \notin S_C,\\ \mathcal{N}\left(\mu_{g,H_1}, \frac{\sigma_{g,H_1}^2}{N}\right) & \text{if } i \in S_C. \end{cases} \qquad (7)
$$

3.2. Analysis of the Detection Statistics

From (7), $T_N^{(i)}$ can be approximated with Gaussian distribution

$$
T_N^{(i)} = \frac{N T_N^{'(i)}}{\sqrt{\|\mathbf{W}^i\|^2}} \sim \begin{cases} \mathcal{N}\left(0, \frac{\sigma_{g,H_0}^2}{\sigma_W^2}\right) & \text{if } i \notin S_C,\\ \mathcal{N}\left(\frac{\sqrt{N}\mu_{g,H_1}}{\sigma_W}, \frac{\sigma_{g,H_1}^2}{\sigma_W^2}\right) & \text{if } i \in S_C. \end{cases} \qquad (8)
$$

The Z statistics can be approximated with a Gaussian random variable $\mathcal{N}(\mu', 1)$ with $\mu' = \frac{1}{2}\sqrt{N-3}\log\frac{1+E[\rho]}{1-E[\rho]}$, where $E[\rho]$ is the mean of ρ defined in (2) and is the correlation coefficient of $\mathbf{Y}$ and $\mathbf{W}^{(i)}$ [1]. Since $E[W^{(i)}] = 0$, we have

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

where $\sigma_{g,Y}^2 = var[g(\{W^{(k)}\}_{k \in S_C})]$ is the variance of the extracted fingerprint. Consequently, we have

$$
\begin{aligned}
Z^{(i)} &\sim \begin{cases} \mathcal{N}(0,\ 1) & \text{if } i \notin S_C,\\ \mathcal{N}\left(\frac{1}{2}\sqrt{N-3}\log\frac{1+E[\rho]}{1-E[\rho]},\ 1\right) & \text{if } i \in S_C, \end{cases}\\
\text{where} \quad E[\rho] &= \frac{E[T_N^{'(i)}]}{\sqrt{\sigma_{g,Y}^2 \sigma_W^2}} = \frac{\mu_{g,H_1}}{\sqrt{\sigma_{g,Y}^2 \sigma_W^2}}. \qquad (9)
\end{aligned}
$$

Similarly, $q^{(i)}$ can be approximated with Gaussian distribution

$$
q^{(i)} \sim \begin{cases} \mathcal{N}(0,\ 1) & \text{if } i \notin S_C,\\ \mathcal{N}\left(\frac{\sqrt{N}\mu_{g,H_1}}{\sqrt{\sigma_{g,H_1}^2}},\ 1\right) & \text{if } i \in S_C. \end{cases} \qquad (10)
$$

[1] Note that the original definition of T_N statistics in [2] is slightly different from the one given here. But it was shown in [6] that this modification is valid for comparing the detection performance of different statistics.

3.3. Analysis of P_d and P_{fp}

Define $\mu_{T_N} \triangleq \frac{\sqrt{N}\mu_{g,H_1}}{\sigma_W}$, $\sigma^2_{T_N,H_1} \triangleq \frac{\sigma^2_{g,H_1}}{\sigma^2_W}$, and $\sigma^2_{T_N,H_0} \triangleq \frac{\sigma^2_{g,H_0}}{\sigma^2_W}$. If the number of colluders is K, among the the M statistics $\{T_N^{(i)}\}_{i=1}^M$, K of them are normally distributed with $\mathcal{N}(\mu_{T_N}, \sigma^2_{T_N,H_1})$, and the others are normally distributed with $\mathcal{N}(0, \sigma^2_{T_N,H_0})$. 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} with

$$\begin{aligned} P_d &= P[\max_{i \in S_C} T_N^{(i)} > h] \approx 1 - (1 - Q(\frac{h - \mu_{T_N}}{\sigma_{T_N,H_1}}))^K, \\ \text{and } P_{fp} &= P[\max_{i \notin S_C} T_N^{(i)} > h] \approx 1 - (1 - Q(\frac{h}{\sigma_{T_N,H_0}}))^{M-K} \end{aligned}$$

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

Define $\mu_Z \triangleq \frac{1}{2}\sqrt{N-3}\log\frac{1+E[\rho]}{1-E[\rho]}$ and $\mu_q \triangleq \sqrt{N}\mu_{g,H_1}/\sqrt{\sigma^2_{g,H_1}}$. Similarly, with a given threshold h, we have

$$\begin{aligned} \text{for the } Z \text{ statistics,} \quad P_d &\approx 1 - (1 - Q(h - \mu_Z))^K, \\ \text{and} \quad P_{fp} &\approx 1 - (1 - Q(h))^{M-K}; \\ \text{for the } q \text{ statistics,} \quad P_d &\approx 1 - (1 - Q(h - \mu_q))^K, \\ \text{and} \quad P_{fp} &\approx 1 - (1 - Q(h))^{M-K}. \end{aligned} \quad (11)$$

4. GAUSSIAN BASED FINGERPRINTS

It was shown in [1] that uniformly distributed fingerprints can be easily defeated by nonlinear collusion attacks. The simulation results in [1] also showed that Gaussian fingerprints are more resistant to nonlinear collusion attacks than uniform fingerprints. However, unlike uniform fingerprints, Gaussian fingerprints are not bounded and may introduce noticeable distortion in the fingerprinted copies. In order to achieve both the robustness against collusion attacks and the imperceptibility of the embedded fingerprints, bounded Gaussian-like fingerprints were introduced in [6].

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^2_W respectively. The pdf of a bounded Gaussian distribution $f'_X(\cdot)$ is:

$$f'_X(x) = \begin{cases} \frac{f_X(x)}{F_X(1) - F_X(-1)} & \text{if } -1 \le x \le 1, \\ 0 & \text{otherwise}. \end{cases} \quad (12)$$

Given the pdf (12) and the analysis in Section 3, we can calculate μ_{g,H_1}, σ^2_{g,H_1}, σ^2_{g,H_0} and $\sigma^2_{g,Y}$, and therefore P_d and P_{fp}. Detailed derivation is available in [6].

From the simulation results in Figure 1, we can see that, three detection statistics have similar performance under the average and randomized negative attacks; and under the minimum and maximum attacks, the Z statistics is more robust than the T_N and q statistics. The detection performance under the maximum attack is the same as that under the minimum attack.

5. PRE-PROCESSING OF THE EXTRACTED FINGERPRINTS

The three detection statistics we have studied so far are not specifically designed for collusion scenarios, and do not exploit the statistical features of the extracted fingerprints under collusion attacks. One of such features is the sample mean of the extracted fingerprints. From the histogram plots of the extracted fingerprints under different attacks as shown in Figure 2, we observe different patterns of the sample means of the extracted fingerprints: the average attack yields an approximately zero sample mean; the minimum and maximum attacks yield a negative and a positive sample means, respectively; and the extracted fingerprint components under the randomized negative attack are from two distributions, one with a negative mean, the other with a positive mean.

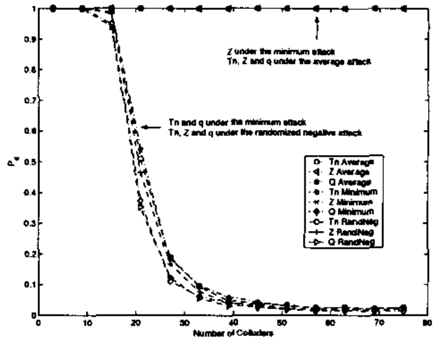

Fig. 1. P_d of three detection statistics under the average, minimum and randomized negative attacks on i.i.d. fingerprints following distribution (12) with $\sigma^2_W = 1/9$. $M = 100$, $N = 10^4$ and $P_{fp} = 10^{-2}$. Results are based on 2000 simulation runs.

Recall from (6) that σ^2_{g,H_0} is proportional to the second moment of the extracted fingerprint, subtracting the sample mean from the extracted fingerprint will reduce its second moment, thus improve the detection performance. Motivated by this intuition, we propose a pre-processing stage in the detection process. Given the extracted fingerprint $\{Y_j = g(\{W_j^k\}_{k \in S_C})\}_{j=1}^N$, we first investigate its histogram. If a single non-zero sample mean is observed, we subtract it from the extracted fingerprint, and then apply the detection statistics. If the fingerprint components are generated from two (or more) distributions, we need to cluster components into different distributions and then subtract the sample mean of each distribution from those fingerprint components in that distribution correspondingly. In our problem, for 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 into the other distribution. Given the extracted fingerprint $\{Y_j\}$, the preprocessing stage generates a new signal $\{Y'_j\}_{j=1}^N$ by

$$Y'_j = \begin{cases} Y_j - \sum_j Y_j \cdot I[Y_j < 0] / \sum_j I[Y_j < 0] & \text{if } Y_j < 0, \\ Y_j - \sum_j Y_j \cdot I[Y_j > 0] / \sum_j I[Y_j > 0] & \text{if } Y_j > 0, \end{cases}$$

where $I[\cdot]$ is the indication function, and then the detector applies the detection statistics to $\{Y'_j\}_{j=1}^N$.

The analysis of the detection statistics with pre-processing is the same as in Section 3. Under the minimum attack, for $i \in S_C$, if $\mu_{min,H_1} = E[W^{min} W^{(i)}]$, $\sigma^2_{min,H_1} = var[W^{min} W^{(i)}]$, $\sigma^2_{min,H_0} = E[(W^{min})^2]\sigma^2_W$, and $\sigma^2_{min,Y} = var[W^{min}]$ are the parameters without pre-processing, then with pre-processing,

$$\begin{aligned} \tilde{\mu}_{min,H_1} &\triangleq E\left[\left(W^{min} - E[W^{min}]\right) W^{(i)}\right] = \mu_{min,H_1}, \\ \tilde{\sigma}^2_{min,H_1} &\triangleq var\left[\left(W^{min} - E[W^{min}]\right) W^{(i)}\right] \\ &= \sigma^2_{min,H_1} + \left(E[W^{min}]\right)^2 \sigma^2_W \\ &\quad -2E\left[W^{min}\right] E\left[W^{min}\left(W^{(i)}\right)^2\right], \end{aligned}$$

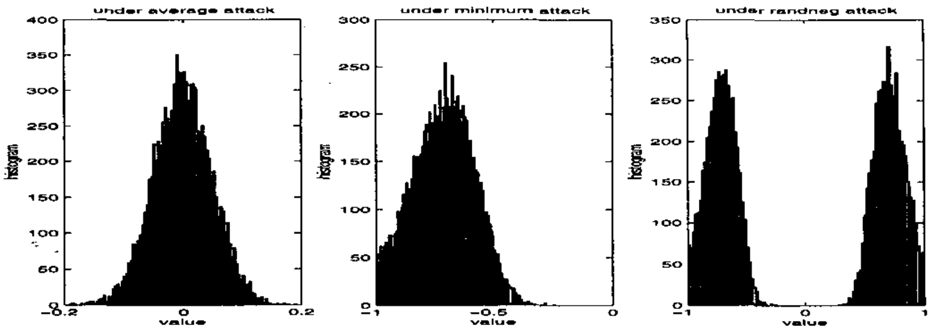

Fig. 2. Histogram of the extracted fingerprints under the average, minimum and randomized negative attacks. Fingerprint components are i.i.d. following distribution (12) with $\sigma_W^2 = 1/9$. $N = 10^4$ and $K = 45$.

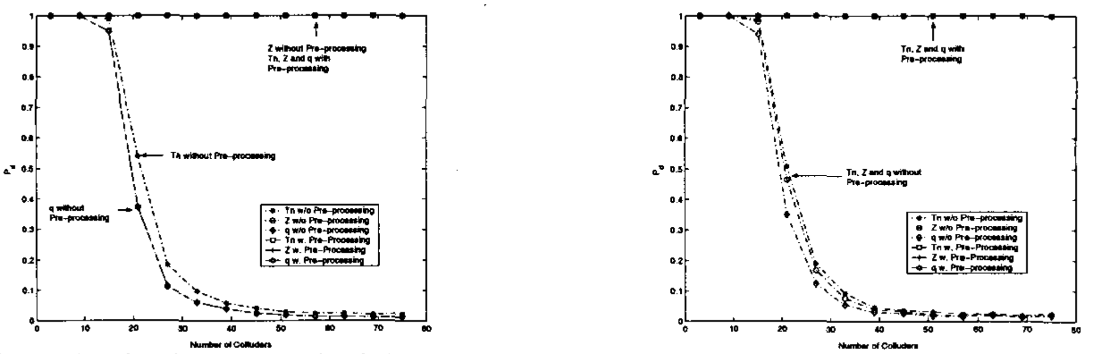

Fig. 3. P_d of the three detection statistics with and without pre-processing under the minimum and randomized negative attacks. Fingerprint components are i.i.d. following distribution (12) with $\sigma_W^2 = 1/9$. $M = 100$, $N = 10^4$and $P_{fp} = 10^{-2}$. Results are based on 2000 simulation runs. Left: under the minimum attack, right: under the randomized negative attack.

$$\bar{\sigma}^2_{min,H_0} \triangleq E\left[\left(W^{min} - E[W^{min}]\right)^2\right]\sigma_W^2 = \sigma^2_{min,Y}\sigma_W^2,$$

$$\text{and } \bar{\sigma}^2_{min,Y} \triangleq var\left[W^{min} - E(W^{min})\right] = \sigma^2_{min,Y}. \qquad (13)$$

The analyses of the maximum and randomized negative attacks are similar and thus omitted here. With (13), the analysis of (P_d, P_{fp}) with this pre-processing stage is the same as in Section 3.3.

The simulation results in Figure 3 show that, with the pre-processing stage, the detection performance under the minimum, maximum and randomized negative attacks is improved, and three statistics have similar performance. The performance under the maximum attack is the same as that under the minimum attack.

6. CONCLUSIONS

In this paper, we have studied the detection performance of commonly used detection statistics on independent Gaussian based fingerprints under collusion attacks. We have shown that, with the three detection statistics as defined in the literature and without any modification, the Z statistics is 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. Observing different patterns of the sample means of the extracted fingerprints under different collusion attacks, we have also introduced a pre-processing stage to improve the detection performance and we have shown that, with the pre-processing stage, the detection performance is improved and the three detection statistics have similar performance under collusion attacks.

Acknowledgement The authors would like to thank Dr. Wade Trappe for his constructive suggestions and inspiring discussions.

7. REFERENCES

[1] H. Stone, "Analysis of attacks on image watermarks with randomized coefficients," Tech. Rep. 96-045, NEC, 1996.

[2] H. V. Poor, *An Introducton to Signal Detection and Estimation*, Springer Verlag, 2nd edition, 1999.

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

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

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

[6] H. Zhao, M. Wu, Z. Jane Wang, and K. J. R. Liu, "Nonlinear collusion attacks on independent multimedia fingerprints," *submitted to IEEE Trans. on Image Proc.*, 2002.

[7] W. Trappe, M. Wu, Z. Jane Wang, and K. J. R. Liu, "Anti-collusion figerprinting for multimedia," *to appear IEEE Tran. on Signal Proc., Sepcial Issues on Signal Proc. for Data Hiding in Digital Media & Secure Content Delivery*, April 2003. A short version appeared in ICASSP'02, vol. 4, pp. 3309 -3312, May 2002.