Optimal detector for multiplicative watermarks embedded in the DFT domain of non-white signals

V. Solachidis and I.Pitas

Department of Informatics, University of Thessaloniki

Thessaloniki 54124, Greece Tel,Fax: +30-2310996304

e-mail: pitas@zeus.csd.auth.gr

Abstract

This paper deals with the statistical analysis of the behavior of a blind robust watermarking system based on pseudorandom signals embedded in the magnitude of the Fourier transform of the host data. The host data that the watermark is embedded into is one-dimensional and non-white, following a specific probability model. The analysis performed involves theoretical evaluation of the statistics of the Fourier coefficients and the design of an optimal detector for multiplicative watermark embedding. Finally, experimental results are presented in order to show the performance of the proposed detector versus that of the correlator detector.

I. Introduction

The risk of illegal copying, reproduction and distribution of copyrighted multimedia material is becoming more threatening with the all-digital evolving solutions adopted by content providers, system designers and users. Thus, copyright watermark protection of digital data is an essential requirement for multimedia distribution. Robust watermarks can offer a copyright protection mechanism for digital media. The watermark is a signal that contains information about the copyright owner and it is embedded permanently in the multimedia data. It introduces imperceptible content changes that can be detected by a detection program.

Robustness is a very important property of the watermarking scheme. The watermarks must be robust to distortions, such as those caused by image processing algorithms (in the case of image watermarks). Image processing does not modify only the image but may also modify the watermark as well. Thus, the watermark may become undetectable after intentional or unintentional image processing attacks. The watermark must also be imperceptible. The watermark alterations should not decrease the perceptual media quality. A general watermarking framework for copyright protection has been presented in [1], [2] and describes all these issues in detail.

Watermarking methods can be distinguished in two major classes, according to the embedding/detection domain. In the first class, the embedding is performed directly in the spatial domain [3]-[5]. The second class is referred to transform domain techniques. In these methods, the watermark is embedded in a transform domain, attempting to exploit the transform properties mainly for watermark imperceptibility and robustness. The watermark can be embedded in the DCT [6]-[9], DFT [10], [11], Fourier-Mellin [12], [13], DWT [7], [14], [15]-[18] or fractal-based coding domains [19], [20]. Many approaches adopt principles from spread spectrum communications in their watermarking system model [8], [21], [1], [2].

Correlation detection of watermarked signals is involved in the majority of the watermarking techniques in the literature. However, correlator detector is optimal and minimizes the error probability only in cases when the signal follows a Gaussian distribution. There are papers in the literature that propose detectors, different than the correlator, in the cases when the host data do not follow a Gaussian distribution [22]-[24]. In [22], the embedding domain is DCT. The DCT coefficient distribution is modelled as a generalized Gaussian one. Then, the maximum likelihood (ML) criterion is used in order to derive the optimal detector structure. In [24], [25], the watermark is embedded in the magnitude of the DFT domain. In this case, the authors assume that the Fourier magnitude does not follow the generalized Gaussian distribution. They propose the Weibull one, due to the facts that its support domain is the set of the positive real numbers and that it represents a big probability distribution family. In the present paper, the watermark is also assumed to be embedded in the magnitude of the DFT domain. Moreover, we assume that the signal is not white and that it follows a specific probability model. The novelty of the present paper, that is also the main difference from the papers reported above, is that the DFT magnitude distribution is analytically calculated and it is proven to be different than the Weibull distribution [24]. Finally, we construct the optimal detector according to the Neyman-Pearson criterion.

The paper is organized as follows. The watermarking system model is presented in section II. In the next section, the signal model is presented and the distribution of DFT magnitude coefficients is shown. Then, in section IV, the construction of the optimal detector is depicted. In sections V and VI, the experimental results and the conclusions are presented.

II. Watermarking system model

Let $s(i),\ i = 1, 2, ..., N$ be the samples of a host signal s with length N. Let also $S(k),\ k = 1, 2, ...N$ be the Discrete Fourier transform coefficients of $s(i)$ and $M(k)$, $P(k)$ the magnitude of the Fourier transform ($M(k) = |S(k)|$) and its phase, $P(k) = \arg(S(k))$, respectively. Suppose that $S_R(k)$ and $S_I(k)$ denote the real and the imaginary part of $S(k)$ respectively. As mentioned in the introduction, the watermark embedding is performed in the Fourier domain and more specifically in its magnitude. Thus, starting from the magnitude of the Fourier transform M, we produce the watermarked transform magnitude. Let us assume that M' is the watermarked magnitude generated by the watermark embedding function f:

$$M' = f(M, W, p). \tag{1}$$

In the previous formula, vector W contains the samples of the watermark sequence. This sequence is produced by a random generator. We assume that $W(k),\ k = 1, 2, ..., N$ is a random signal that consists solely of $1'$s and $-1'$s and that it is uniformly distributed in its domain $\{1, -1\}$. Thus, the mean of the watermark sequence samples $W(k)$ is equal to zero. In the case that f is of a linear form, it can be easily proven that the mean of the watermarked magnitude remains unaltered. This property increases both the watermarked signal imperceptibility as well as its robustness. The parameter p that is employed in (1) is a real number that determines the watermark strength. An increase in the value of p results in a more robust (and more easily perceptible) watermark.

If the embedding function is multiplicative, the watermarked magnitude is given by:

$$M' = M + MWp = M(1 + Wp). \tag{2}$$

In order to compute the final watermarked signal s' (in the spatial domain), the inverse discrete

Fourier transform is applied on the watermarked magnitude M' and the initial DFT coefficient phase P.

$$s' = IDFT(M', P). \tag{3}$$

Given a possibly watermarked signal y, the watermark detector aims at deciding whether y hosts a certain watermark W. Watermark detection can be expressed as a hypothesis test where two hypotheses are possible:

- H_0: signal y does not host watermark W
- H_1: signal y hosts watermark W.

It should be noted that hypothesis H_0 can occur either in the case that the signal y is not watermarked (hypothesis H_{0a}) or in the case that the signal y is watermarked by another watermark W', where $W \neq W'$ (hypothesis H_{0b}). The events H_{0a}, H_{0b} are mutually exclusive and their union produces the hypothesis H_0.

The performance of a watermarking method depends mainly on the selection of the watermark detector d. The correlator detector is the most commonly used watermark detector. It has been employed in many watermarking methods which perform not only spatial domain watermarking but also watermarking in transform domains. Its test statistic is the correlation between the watermark and the possibly watermarked signal y.

$$d = \frac{1}{N} \sum_{i=1}^{N} y(i)W(i) \tag{4}$$

In order to decide on the valid hypothesis, the detector output d is compared against a suitably selected threshold T. The evaluation of the watermarking method can be measured by the false alarm P_{fa} and the false rejection P_{fr} probabilities. False alarm probability is the type I error which is the probability of rejecting hypothesis H_0, even though it is true. In our case it is the probability of detecting a watermark W in a signal that is not watermarked by the watermark

W. Correspondingly, false rejection is the type II error, whose probability is that of not detecting a watermark W in a signal that is actually watermarked by the watermark W (accept H_0 even it is false).

In most of the watermarking methods, hypothesis H_0 is accepted, when the detector output is greater than a threshold T. Thus, false alarm and false rejection probabilities can be expressed as:

$$P_{fa} = P\{d > T|H_0\}, P_{fr} = P\{d < T|H_1\}.$$

The calculation of the above probabilities can be performed, if the detector distribution for both hypotheses is known. Thus, assuming that the $f_0(x)$, $f_1(x)$ are the probability density functions for the hypotheses H_0 and H_1 respectively, the error probabilities are given by:

$$P_{fa} = \int_T^\infty f_1(x)dx,$$

$$P_{fr} = \int_\infty^T f_0(x)dx.$$

According to the above equations, P_{fa} and P_{fr} depend on the threshold T. A possible change of T increases one probability and decreases the other. Thus, apart from the detector, an appropriate threshold should be selected. In many cases the detector is expressed as a sum or a product of almost independent terms that obey the same distribution. According to the central limit theorem, the detector (or the detector logarithm in case of multiplicative embedding) obey a Gaussian distribution. Thus, in this case, the error probabilities can be written as

$$P_{fa} = f(\frac{T-\mu_1}{\sigma_1}),$$

$$P_{fr} = 1 - f(\frac{T-\mu_0}{\sigma_0}),$$

$$f(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} exp\left(\frac{-x^2}{2}\right)$$

where μ_0, μ_1 are the mean values and σ_0, σ_1 the standard deviations of the distributions f_0, f_1 respectively.

III. Signal model and distribution of DFT magnitude coefficients

A basic step for the optimal detector construction is the computation of the transform coefficient distribution. Thus, in this section, the distribution of the DFT magnitude coefficients of a signal will be computed, whose model is ergodic and wide-sense stationary stochastic process. The signal statistics are modeled as:

$$E(s(i)) = \mu_s, \ \forall i = 0, ..., N-1 \tag{5}$$

$$E(s(i)\ s(i+D)) = F_{s,s}(D), \ \forall i = 0, ..., N-1 \tag{6}$$

$$\sigma_s^2 = E(s(i)^2) - \mu_s^2 \tag{7}$$

where $E(\cdot)$ denotes the expected value.

A first order separable autocorrelation function model will be assumed [26]:

$$F_{s,s}(D) = \mu_s^2 + \sigma_s^2 a^{|D|} \tag{8}$$

where a is a real-valued constant. Typically a is in the range $[a = 0.9, ...0,99]$ for several class of 1D signals (e.g. audio). It should be noted that if a tends to zero, the autocorrelation approaches a Dirac distribution.

It is obvious from equations (5) and (8) that the signal correlation $F_{s,s}(D)$ depends only on the absolute difference D of the signal indices. The DFT transform of signal $s(i),\ i = 1, ..., N$ is given by the following equation:

$$S(k) = \sum_{i=0}^{N-1} s(i) e^{-\frac{j2\pi ik}{N}} = \sum_{i=0}^{N-1} s(i) \cos\left(\frac{-2\pi ik}{N}\right) + j s(i) \sin\left(\frac{-2\pi ik}{N}\right),\ k = 1, ..., N \tag{9}$$

We can assume that the DFT transform (9) of the signal follow a Gaussian distribution due the Central Limit Theorem for random variables with small dependency [27]. This assumption is valid at least for small values of parameter a. In order to show this experimentally we have performed the Kolmogorov-Smirnov test for all the coefficients. In Figure 2 the p-values for each coefficient for the case of $a = 0$ (Figure 2a) and $a = 0.995$ (Figure 2b) are illustrated. The statistic parameters used in the Kolmogorov-Smirnov test (expected value and variance) were theoretically derived from equations 12, 13, and 30. It is shown that the p-values are very low which means that all the coefficients follow the Gaussian distribution.

Thus, it is proved that the mean of $S(k)$ is given by:

$$\mu_{S(k)} = E[S(k)] = E\left[\sum_{i=0}^{N-1} s(i)e^{-\frac{j2\pi ik}{N}}\right] = \begin{cases} 0, & k \neq 0 \\ \mu_s N, & k = 0. \end{cases}$$

The proof of $\mu_{S(k)}$ is given in the Appendix. The variance of $S(k)$ will be computed separately for its real $S_R(k)$ and imaginary $S_I(k)$ part according to the following formula:

$$\begin{aligned} \sigma^2_{S_R(k)} &= E[S_R(k)^2] - E[S_R(k)]^2 = \\ &= \sum_{i=0}^{N-1}\sum_{l=0}^{N-1} \cos\left(\frac{-2\pi ik}{N}\right)\cos\left(\frac{-2\pi lk}{N}\right) E[s(i)s(l)] - \mu^2_{S_R(k)} \end{aligned} \tag{10}$$

By substituting equation (5) in the equation (10) we result in

$$\sigma^2_{S_R(k)} = \sum_{i=0}^{N-1}\sum_{l=0}^{N-1} \cos\left(\frac{-2\pi ik}{N}\right)\cos\left(\frac{-2\pi lk}{N}\right)\left(m^2 + s^2 a^{|j-m|}\right) - \mu^2_{S_R(k)} \tag{11}$$

The final results for the variances of $S_R(k)$ and $S_I(k)$ are given below:

$$\sigma^2_{S_R(k)} = -\frac{1}{2}s^2 \frac{\left(\begin{array}{l} -2a\cos\left(2\frac{\pi k}{N}\right)\left(2a^N(1+a^2) + a^2(N-2) - N - 2\right) \\ -N + a^4 N - 6a^2 + 6a^2 a^N + 2a^2\cos\left(4\frac{\pi k}{N}\right)\left(a^N - 1\right) \end{array}\right)}{2a^2\cos\left(4\frac{\pi k}{N}\right) + 4a^2 - 4a\cos\left(2\frac{\pi k}{N}\right)(1+a^2) + 1 + a^4} \tag{12}$$

$$\sigma^2_{S_I(k)} = -\frac{1}{2}s^2 \frac{\left(-2a^2\cos\left(4\frac{\pi k}{N}\right)\left(a^N-1\right) - 2aN\cos\left(2\frac{\pi k}{N}\right)(a^2-1) + N(a^4-1) + 2a^2(a^N-1)\right)}{2a^2\cos\left(4\frac{\pi k}{N}\right) + 4a^2 - 4a\cos\left(2\frac{\pi k}{N}\right)(1+a^2) + 1 + a^4} \tag{13}$$

The proof of the above equations is given in the Appendix.

In Figure 1 the theoretical variances and experimental of real and imaginary part of the Discrete Fourier transform coefficients are shown. In this example 100 signals of length 1000 obeying the model (8) were used for $a = 0,99$.

The next step is to calculate the distribution of the Fourier magnitude $|S(k)|$. By observing (10), we conclude that all but the DC term, have zero mean. If the variances of $S_R(k)$ and $S_I(k)$ were equal, then we could conclude that the distribution of $|S(k)| = \sqrt{S_R(k)^2 + S_I(k)^2}$ is the Rayleigh one [28]:

$$|S(k)| \sim f_s(s) = \frac{s}{\sigma^2}\exp\left(-\frac{s^2}{2\sigma^2}\right),\ x > 0.$$

However, the variances of the real and the imaginary part of $S(k)$ are equal only in the case of signals whose samples can be modeled as independent identically distributed (i.i.d) random variables ($a = 0$). Thus, for any other case we have to use the probability density function of a signal

$$z = \sqrt{x^2 + y^2}$$

where $x \sim N(0, \sigma_1^2)$, $y \sim N(0, \sigma_2^2)$ and $\sigma_1 \neq \sigma_2$. It is proved in the Appendix that the pdf of such a random variable z is given by:

$$f_z(z) = \frac{z}{\sigma_1\sigma_2}\exp\left(-\frac{\sigma_1^2+\sigma_2^2}{4\sigma_1^2\sigma_2^2}z^2\right) I_0\left(0, \frac{\sigma_2^2-\sigma_1^2}{4\sigma_1^2\sigma_2^2}z^2\right) \tag{14}$$

where I_0 denotes the modified Bessel function and σ_1, σ_2 are the standard deviations of the real

and imaginary part of $S(k)$. Thus, the Discrete Fourier magnitude distribution is given by:

$$|S(k)| \sim f_z(z) = \frac{z}{2\sigma_{S_{R(k)}}\sigma_{S_{I(k)}}} \exp\left(-\frac{\sigma^2_{S_{R(k)}} + \sigma^2_{S_{I(k)}}}{4\sigma^2_{S_{R(k)}}\sigma^2_{S_{I(k)}}} z^2\right) I_0\left(0, \frac{\sigma^2_{S_{I(k)}} - \sigma^2_{S_{R(k)}}}{4\sigma^2_{S_{R(k)}}\sigma^2_{S_{I(k)}}} z^2\right). \quad (15)$$

IV. Optimal watermark detector

In the next section the optimal watermark detector for multiplicative watermarks will be evaluated by using the likelihood ratio test (LTR). According to the Neyman-Pearson theorem, in order to maximize the probability of detection P_D for a given $P_{fa} = e$, we decide for H_1 if:

$$L(M') = \frac{p(M'; H_1)}{p(M'; H_0)} > T \quad (16)$$

where the threshold T can be found from

$$P_{fa} = \int_{M':L(M')>T} p(M'; H_0) dM' = e \quad (17)$$

The test of (16) is called Likelihood Ratio Test (LTR). In the sequel the probability density functions of the watermarked signal $P(M'; H_0), P(M'; H_1)$ will be computed for watermarked signals with a known and an unknown (random) watermark. For $P(M'; H_0)$ we assume that the watermark is a random one whose pdf is modeled by:

$$f_w(w) = \begin{cases} 0.5 & , w = 1 \\ 0.5 & , w = -1 \\ 0 & , otherwise \end{cases} \quad (18)$$

According to the embedding formula (2), it can be easily proved that the pdf of the watermarked signal is equal to:

$$f_{M'}(x) = \frac{1}{2}\left[\frac{1}{1+p}\, f_M\left(\frac{x}{1+p}\right) + \frac{1}{1-p}\, f_M\left(\frac{x}{1-p}\right)\right] \quad (19)$$

By substituting f'_M with the probability density function of the distribution in equation (14) we find:

$$p(M';H_0) = \frac{M'(k)}{4\sigma_1\sigma_2} \cdot \tag{20}$$
$$\left[\frac{1}{(1+p)^2}\exp\left(-\frac{\sigma_1^2+\sigma_2^2}{4\sigma_1^2\sigma_2^2}\frac{M'(k)^2}{(1+p)^2}\right) I_0\left(0, \frac{\sigma_2^2-\sigma_1^2}{4\sigma_1^2\sigma_2^2}\frac{M'(k)^2}{(1+p)^2}\right) + \right.$$
$$\left.\frac{1}{(1-p)^2}\exp\left(-\frac{\sigma_1^2+\sigma_2^2}{4\sigma_1^2\sigma_2^2}\frac{M'(k)^2}{(1-p)^2}\right) I_0\left(0, \frac{\sigma_2^2-\sigma_1^2}{4\sigma_1^2\sigma_2^2}\frac{M'(k)^2}{(1-p)^2}\right)\right]$$

In the case of hypothesis H_1, the signal is watermarked by the known watermark W. Thus, the probability is given by (14):

$$p(M'(k);H_1) = \frac{M'(k)}{2\sigma_1\sigma_2(1+W(k)p)^2}$$
$$\exp\left(-\frac{\sigma_1^2+\sigma_2^2}{4\sigma_1^2\sigma_2^2}\frac{M'(k)^2}{(1+W(k)p)^2}\right) I_0\left(0, \frac{\sigma_2^2-\sigma_1^2}{4\sigma_1^2\sigma_2^2}\frac{M'(k)^2}{(1+W(k)p)^2}\right). \tag{21}$$

Assuming independence between the transform coefficients of S, we conclude that:

$$p(M';H_j) = \prod_{k=0}^{N-1} p(M'(k);H_j) \quad , j = 0,1 \tag{22}$$

By combining equations (14), (21) and (16) we get the optimal detector scheme:

$$L(M') = \prod_{k=1}^{N-1} \frac{\frac{2}{(1+W(k)p)^2} I_0\left(0, \frac{\sigma_2^2-\sigma_1^2}{4\sigma_1^2\sigma_2^2}\frac{M'(k)^2}{(1+W(k)p)^2}\right)}{\frac{1}{(1+p)^2}\exp\left(-\frac{\sigma_1^2+\sigma_2^2}{4\sigma_1^2\sigma_2^2}\frac{2p(W(k)-1)M'(k)^2}{(1+W(k)p)^2(1+p)^2}\right) I_0\left(0, \frac{\sigma_2^2-\sigma_1^2}{4\sigma_1^2\sigma_2^2}\frac{M'(k)^2}{(1+p)^2}\right) + \frac{1}{(1-p)^2}\exp\left(-\frac{\sigma_1^2+\sigma_2^2}{4\sigma_1^2\sigma_2^2}\frac{2p(W(k)+1)M'(k)^2}{(1+W(k)p)^2(1-p)^2}\right) I_0\left(0, \frac{\sigma_2^2-\sigma_1^2}{4\sigma_1^2\sigma_2^2}\frac{M'(k)^2}{(1-p)^2}\right)} > T \tag{23}$$

A. Threshold estimation

The threshold is selected in such a way so that a predefined false alarm error probability can be achieved. In order to calculate the false alarm error probability, we firstly have to know the detector distribution in the case of erroneous watermark detection. We assume that the

distribution is Gaussian. Then, we estimate the distribution parameters from the statistics of the empirical distribution. The latter is calculated by detecting erroneous watermarks from the (possibly) watermarked signal.

From the empirical distribution statistics and the desired false alarm error probability, we calculate the threshold according the equation below:

$$P_{fa} = \int_{T}^{+\infty} \frac{1}{\widehat{\sigma}\sqrt{2}} \exp\left(-\frac{(x-\widehat{\mu})^2}{2\widehat{\sigma}^2}\right) dx \tag{24}$$

where $\widehat{\mu}$ and $\widehat{\sigma}$ are the expected value and the standard deviation of the detector output set. Thus, according to the equation above, the threshold T is given by:

$$T = \widehat{\mu} - \widehat{\sigma}\sqrt{2}\ \ erf^{-1}(2\ P_{fa} - 0.5) \tag{25}$$

The total number of such detections needed is not predefined but, should be sufficiently large if we want to accurately approximate this distribution. The minimal number of experiments required in order to sufficiently approximate the distribution is found through the following procedure. We estimate the distribution parameters, $\widehat{\mu}$, $\widehat{\sigma}$ using the empirical distribution produced from L detector outputs, for an increasing L in a certain range of L, $[L_{min}, L_{max}]$. Then, according to these statistics, we calculate the threshold in order to achieve a false alarm probability e.g. equal to 10^{-10}. We stop for an L^* that leads a rather stable estimation of T.

This procedure is illustrated in Figure 4 for $L_{min} = 5$, $L_{max} = 1000$. According to this Figure, the threshold value is stabilized when the number of experiments becomes greater than $L^* = 100$. Of course, L^* depends on the watermark embedding power, the signal length, and the signal characteristics. For this reason, we propose to execute the above procedure for representative signal sets and for the chosen embedding power in a particular application.

V. Experimental results

In this section, experiments are performed in order to verify the superiority of the proposed detector against the classical correlator one. The experiments are performed on one dimensional digital signals.

In order to construct signals with the desired autocorrelation properties (8) we filter a random white normally distributed signal S of zero mean value with an IIR filter:

$$H(z) = \frac{1-a}{1-az^{-1}}.$$

This filtering creates a signal having an autocorrelation function of the form:

$$R_{SS}(k) = \frac{1-b}{1+b}\sigma_s^2 a^k \tag{26}$$

that is identical to (8) for $\mu_s^2 = 0$. The variance of the filtered signal equals to $(1-a)/(1+a)\sigma_s^2$. Watermark embedding is performed according to (2). Then, the watermarked signal is fed to both the correlator (4) and the proposed detectors (23). In order to estimate false alarm and false rejection probabilities, both correct and erroneous keys have been used during detection.

The above procedure is executed for a large number of different keys. Due to the Central Limit Theorem for products [29], the distribution of $L(x)$ is log-normal. Consequently, the distribution of $\ln(L(x))$ is normal, where $\ln(x)$ is the natural logarithm of x. In order to show the very good approximation of the detector output by the Gaussian distribution, we depict its empirical distribution in Figure 3. In Figures 3a and 3b the detector distribution for detection using an erroneous and correct key respectively is shown. The fitting is very good since the Kolmogorov-Smirnov null hypothesis has not been rejected for level of significance equal to 0.01 In the following the proposed detector will be the $\ln(L(x))$ instead of $L(x)$. Let $dr(x)$ and $de(x)$ be the distributions of the detector outputs for detecting correct and erroneous watermarks respectively.

The calculation of the empirical mean and standard deviation by approximating the empirical pdf with a normal one, can be used to produce Receiver Operator Characteristic (ROC) curves for both detector outputs. ROC curves will be used for comparing detector performance.

The above procedure is performed for several values of parameter a. The detection was performed using:

- the correlator detector
- the proposed detector considering the parameter a known
- the proposed detector by estimating the (unknown) parameter a from the watermark sequence
- the normalized correlator

In Figures 5-8 the performance of the proposed detector against the correlator one is shown, for several values of parameter a in the range $[0, 1]$.

In Figure 5, the value of the parameter a is zero. This is a special case for white signals, i.e. no filtering is performed by equation(26). In the subsequent Figures, the parameter a increases, reaching the value $a = 0.995$ in the last Figure (Figure 8). By observing the Figures 5-8, we can conclude that:

- the proposed detector performance is by far better that the correlator detector one.
- The performance of the proposed detector using the estimated parameter a, is almost the same with that using the known parameter a since that their ROC curves are very close to each other
- The ROC curves that correspond to the proposed detector are not affected significantly by the value parameter a contrary to the correlator detect or ROC curves that show very decreased detection performance for highly correlated signals, i.e. as parameter a tends to one.

VI. Conclusions and future work

This paper deals with the statistical analysis of the behavior of a blind robust watermarking system based on 1-D pseudorandom signals embedded in the magnitude of the Fourier transform of the data and the design of an optimum detector. A multiplicative embedding method is examined and experiments are performed in order to show the proposed detector's improved efficiency against correlator one.

Appendix

I. Calculation of Discrete Fourier coefficient mean

The mean of $S(k)$ is given by:

$$\begin{aligned} E\left[S(k)\right] &= E\left[\sum_{i=0}^{N-1} s(i)\cos\left(\frac{-2\pi ik}{N}\right) + js(i)\sin\left(\frac{-2\pi ik}{N}\right)\right] \\ &= E[s(i)]\sum_{i=0}^{N-1}\cos\left(\frac{-2\pi ik}{N}\right) + jE(s(i))\sum_{i=0}^{N-1}\sin\left(\frac{-2\pi ik}{N}\right) \end{aligned} \tag{27}$$

Replacing na by $\frac{2\pi kj}{N}$ in the following equation [30]

$$\sum_{n=1}^{N}\cos(na) = \begin{cases} \frac{\sin[(N+1/2)a]}{2\sin(a/2)} - \frac{1}{2}, a \neq 2l\pi \\ N, a = 2l\pi \end{cases}$$

results in

$$\sum_{j=0}^{N-1}\cos(\frac{2\pi kj}{N}) = 1 + \sum_{j=1}^{N-1}\cos(\frac{2\pi kj}{N}) = 1 + \begin{cases} \frac{\sin\left[(N-1+1/2)\frac{2\pi k}{N}\right]}{2\sin(\frac{\pi k}{N})} - \frac{1}{2}, k \neq 0 \\ N-1, k = 0 \end{cases}$$

Taking into account that $0 \leq k < N$ equation the constraint $a \neq 2l\pi$ can be written as $\frac{2\pi k}{N} \neq 2l\pi \Rightarrow k \neq 0$

Finally

$$\sum_{j=0}^{N-1}\cos\left(\frac{2\pi kj}{N}\right) = \begin{cases} 0, k \neq 0 \\ N, k = 0 \end{cases} \tag{28}$$

Using the equation

$$\sum_{n=1}^{N}\sin(na) = \begin{cases} \frac{\sin[1/2(N+1)a]\sin[Na/2]}{\sin(a/2)}, a \neq 2l\pi \\ 0, a = 2l\pi \end{cases}$$

and following the same procedure we end up in the following equation

$$\sum_{j=0}^{N-1}\sin\left(\frac{2\pi kj}{N}\right) = 0 \tag{29}$$

Thus, the mean is equal to:

$$\mu_{S(x)} = E[S(x)] = \begin{cases} 0, & k \neq 0 \\ E[s(i)]N, & k = 0 \end{cases} \tag{30}$$

II. Calculation of Discrete Fourier coefficient variance

$S(k)$ is a complex signal thus the variances of real and imaginary part will be calculated separately.

A. Variance of real part

The variance of the real part of $S(k)$ is given by:

$$\begin{aligned} var(S_R(k)) &= E(S_R^2(k)) - E(S_R(k))^2 \\ &= E\left[\left(\sum_{i=0}^{N-1} s(i)\cos\left(\frac{-2\pi ik}{N}\right)\right)^2\right] - E\left[\sum_{i=0}^{N-1} s(i)\cos\left(\frac{-2\pi ik}{N}\right)\right]^2 \end{aligned} \tag{31}$$

The second sum has been calculated in 30. The first sum equals to:

$$\begin{aligned} E\left[\left(\sum_{i=0}^{N-1} s(i)\cos\left(\frac{-2\pi ik}{N}\right)\right)^2\right] &= \sum_{i=0}^{N-1}\sum_{m=0}^{N-1}\cos\left(\frac{2\pi ik}{N}\right)\cos\left(\frac{2\pi mk}{N}\right)E[s(i)s(m)] \\ &= \sum_{i=0}^{N-1}\sum_{m=0}^{N-1}\cos\left(\frac{2\pi ik}{N}\right)\cos\left(\frac{2\pi mk}{N}\right)(\mu_s^2 + \sigma_s^2 a^{|i-m|})] = \end{aligned} \tag{32}$$

Using the equation 3 of 1.353 of [31]

$$\sum_{k=0}^{n-1} p^k\cos(ks) = \frac{1 - p\cos(s) - p^n\cos(ns) + p^{n+1}\cos(n-1)s}{1 - 2p\cos(s) + p^2} \tag{33}$$

and splitting the sum $\sum_{m=0}^{N-1}\cos\left(\frac{2\pi ik}{N}\right)\cos\left(\frac{2\pi mk}{N}\right)(\mu_s^2 + \sigma_s^2 a^{|i-m|})]$ in two sums

$$\begin{aligned} &\sum_{m=0}^{N-1}\cos\left(\frac{2\pi ik}{N}\right)\cos\left(\frac{2\pi mk}{N}\right)(\mu_s^2 + \sigma_s^2 a^{|i-m|})] = \\ &\sum_{m=0}^{i}\cos\left(\frac{2\pi ik}{N}\right)\cos\left(\frac{2\pi mk}{N}\right)(\mu_s^2 + \sigma_s^2 a^{i-m})] + \end{aligned}$$

$$\sum_{m=i+1}^{N-1} \cos\left(\frac{2\pi ik}{N}\right) \cos\left(\frac{2\pi mk}{N}\right) (\mu_s^2 + \sigma_s^2 a^{m-i})] \tag{34}$$

we derive equation 12.

B. Variance of imaginary part

The variance of the imaginary part of $S(k)$ is given by:

$$\begin{aligned} var(S_I(k)) &= E(S_I^2(k)) - E(S_I(k))^2 \\ &= E\left[\left(\sum_{i=0}^{N-1} s(i) \sin\left(\frac{-2\pi ik}{N}\right)\right)^2\right] - E\left[\sum_{i=0}^{N-1} s(i) \sin\left(\frac{-2\pi ik}{N}\right)\right]^2 \end{aligned} \tag{35}$$

By splitting the above equation as in 34 and using the equation 1 of 1.353 of [31] that has the form:

$$\sum_{k=1}^{n-1} p^k \sin(kx) = \frac{p\sin(x) - p^n \sin(nx) + p^{n+1}\sin(n-1)x}{1 - 2p\sin(x) + p^2} \tag{36}$$

we conclude in equation 13.

III. Calculation of the $f_z(z)$ distribution

In this section the distribution of $f_z(z) = \sqrt{x^2 + y^2}$, where $x \sim N(0, \sigma_1^2)$, $y \sim N(0, \sigma_2^2)$ and $\sigma_1 \neq \sigma_2$, will the calculated. By substituting x by $z\cos(t)$ and y by $z\sin(t)$ the above distribution equals with:

$$\begin{aligned} f(z) &= \int_0^{2\pi} \frac{z}{2\pi\sigma_1\sigma_2} \exp\left[-\left(\frac{z^2\cos^2(t)}{2\sigma_1^2} + \frac{z^2\sin^2(t)}{2\sigma_2^2}\right)\right] dt = \\ &\int_0^{2\pi} \frac{z}{2\pi\sigma_1\sigma_2} \exp\left[-\left(\frac{z^2\cos^2(t)}{2\sigma_1^2} + \frac{\left(\frac{\sigma_2}{\sigma_1}\right)^2 z^2\sin^2(t)}{2\sigma_2^2} + \frac{\left[1 - \left(\frac{\sigma_2}{\sigma_1}\right)^2\right] z^2\sin^2(t)}{2\sigma_2^2}\right)\right] dt = \\ &\int_0^{2\pi} \frac{z}{2\pi\sigma_1\sigma_2} \exp\left(-\frac{z^2}{2\sigma_1^2}\right) \exp\left[-\frac{\left[1 - \left(\frac{\sigma_2}{\sigma_1}\right)^2\right] z^2\sin^2(t)}{2\sigma_2^2}\right] dt \end{aligned} \tag{37}$$

By substituting the quantity $-\frac{\left[1-\left(\frac{\sigma_2}{\sigma_1}\right)^2\right]}{2\sigma_2^2} = \frac{\sigma_2^2-\sigma_1^2}{2\sigma_1^2\sigma_2^2}$ by the parameter q equation 37 has the form:

$$f(z) = \frac{z}{2\pi\sigma_1\sigma_2}\exp\left(-\frac{z^2}{2\sigma_1^2}\right)\int_0^{2\pi}\exp\left[qz^2\sin^2(t)\right]dt \tag{38}$$

After taking into account the periodicity of the sin function and its symmetry in the integral $[0, 2\pi]$ ($\int_0^{2\pi}\exp\left(a\sin^2(t)\right)dt = 2\int_0^{\pi}\exp\left(a\frac{1-\cos(2t)}{2}\right)dt = \exp\left(\frac{a}{2}\right)\int_0^{2\pi}\exp\left(\frac{-a}{2}\cos(t)\right)dt =$
$2\exp\left(\frac{a}{2}\right)\int_0^{\pi}\exp\left(\frac{-a}{2}\cos(t)\right)dt$)

the integral in equation 38 can be written as

$$\int_0^{2\pi}\exp\left[qz^2\sin^2(t)\right]dt = 2\exp\left(\frac{qz^2}{2}\right)\int_0^{\pi}\exp\left[-\frac{qz^2}{2}\cos(t)\right]dt \tag{39}$$

Using the formula 3.339 of [31]

$$\int_0^{\pi}\exp\left[z\cos(x)\right]dx = \pi I_0(z) \tag{40}$$

where $I_0(z)$ is the modified Bessel function of z, the integral in equation 39 equals:

$$\int_0^{2\pi}\exp\left[-\frac{qz^2}{2}\cos(t)\right]dt = 2\pi\exp\left(\frac{qz^2}{2}\right)I_0\left(-\frac{qz^2}{2}\right) \tag{41}$$

Finally, substituting q and using equation 41, equation 38 has the form:

$$f(z) = \frac{z}{\sigma_1\sigma_2}\exp\left(-\frac{z^2(\sigma_1^2+\sigma_2^2)}{4\sigma_1^2\sigma_2^2}\right)I_0\left(\frac{z^2(\sigma_1^2-\sigma_2^2)}{4\sigma_1^2\sigma_2^2}\right) \tag{42}$$

In the special case that $\sigma_1 = \sigma_2$, the probability density function $f(z)$ is the Rayleigh function.

References

[1] G. Voyatzis and I. Pitas, "Protecting digital-image copyrights: A framework," *IEEE Computer Graphics and Applications*, vol. 19, no. 1, pp. 18–24, January/February 1999.

[2] G. Voyatzis and I. Pitas, "The use of watermark in the rotection of digital multimedia products," *IEEE Proceedings Special issue on Identification and protection of multimedia information*, vol. 87, no. 7, pp. 1197–1207, July 1999.

[3] M.D. Swanson, B.Zhu, A.H. Tewfik, and L. Boney, "Robust audio watermarking using perceptual masking," *Elsevier Signal Processing, Sp. Issue on Copyright Protection and Access control*, vol. 66, no. 3, pp. 337–355, 1998.

[4] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," *Elsevier Signal Processing, Sp. Issue on Copyright Protection and Access control*, vol. 66, no. 3, pp. 385–403, May 1998.

[5] I. Pitas, "A method for watermark casting in digital images,," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 8, no. 6, October 1998.

[6] M. Barni, F. Bartolini, V. Cappelini, and A. Piva, "A DCT-domain system for robust image watermarking," *Elsevier Signal Processing*, vol. 66, no. 3, pp. 357–372, 1998.

[7] R.B. Wolfgang, C.I. Podilchuk, and E.J. Delp, "Perceptual watermarks for digital images and video," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1108–1126, July 1999.

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

[9] A.G. Bors and I. Pitas, "Image watermarking using block site selection and D.C.T. domain constraints," *Optics Express*, vol. 3, no. 12, pp. 512–523, July 1998.

[10] M. Kutter, F. Jordan, and F. Bossen, "Digital watermarking of color images using amplitude modulation," *SPIE Journal of Electronic Imaging*, vol. 7, no. 2, pp. 326–332, 1998.

[11] V.Solachidis and I.Pitas, "Circularly symmetric watermark embeddong in 2-d dft domain," *IEEE Transactions on Image Processing*, vol. 10, no. 11, pp. 1741–1753, 2001.

[12] J.K. Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Elsevier Signal Processing, Sp. Issue on Copyright Protection and Access control*, vol. 66, no. 3, pp. 303–317, 1998.

[13] S. Pereira, J. Ruanaidh, F. Deguillaume, G. Csurka, and T. Pun, "Template based recovery of fourier-based

watermarks using log-polar and log-log maps," in *Proc. of ICMCS'99*, Florence, Italy, 7-11 June 1999, vol. I, pp. 870–874.

[14] M.D. Swanson, B. Zhu, and A.H. Tewfik, "Multiresolution scene-based video watermarking using perceptual models," *IEEE Journal of Selected Areas of Communications*, vol. 16, no. 4, pp. 540–550, May 1998.

[15] C.I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 525–539, May 1998.

[16] M. Barni, F. Bartolini, V. Cappellini, A. Lippi, and A. Piva, "A DWT-based technique for spatio-frequency masking of digital signatures," in *Proc. of SPIE Electronic Imaging'99, Security and Watermarking of Multimedia Contents*, 25-27 January 1999, vol. 3657.

[17] D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1167–1180, July 1999.

[18] S. Tsekeridou and I. Pitas, "Embedding self-similar watermarks in the wavelet domain," in *Proc. of ICASSP'00*, Istanbul, Turkey, 5-9 June 2000, to appear.

[19] J. Puate and F. Jordan, "Using fractal compression scheme to embed a digital signature into an image," in *Proc. of SPIE Photonics East Symposium*, Boston, USA, 18-22 November 1996.

[20] P. Bas, J.-M. Chassery, and F. Davoine, "Using the fractal code to watermark images," in *Proc. of ICIP'98*, Chicago, Illinois, USA, 4-7 October 1998, vol. I, pp. 469–473.

[21] F. Hartung, J.K. Su, and B. Girod, "Spread spectrum watermarking: Malicious attacks and counter-attacks," in *Proc. of SPIE: Security and Watermarking of Multimedia Contents*, California, USA, January 1999, vol. 3657.

[22] Juan R. Hernandez, Martin Amado, and Fernando Perez-Gonzalez, "Dct-domain watermarking techniques for still images: Detector performance analysis and a new structure," *IEEE Transactions on Image Processing*, vol. 9, no. 1, pp. 55–68, January 2000.

[23] M.Barni, F.Bartolini, A.DeRosa, and A.Piva, "Optimum decoding and detection of multiplicative watermarks," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 1118–1123, April 2003.

[24] M.Barni, F.Bartolini, A.DeRosa, and A.Piva, "A new decoder for the optimum recovery of nonadditive watermarks," *IEEE Transactions on Image Processing*, vol. 10, no. 5, pp. 755–766, May 2001.

[25] Qiang Cheng and T.S. Huang, "Robust optimum detection of transform domain multiplicative watermarks," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 906–924, April 2003.

[26] Jean-Paul Linnartz, Ton Kalker, and Geert Depovere, "Modeling the false alarm and missed detection rate for electronic watermarks," in *Proceedings of second Information Hiding Workshop*, Oregon,USA, pp. 329–343.

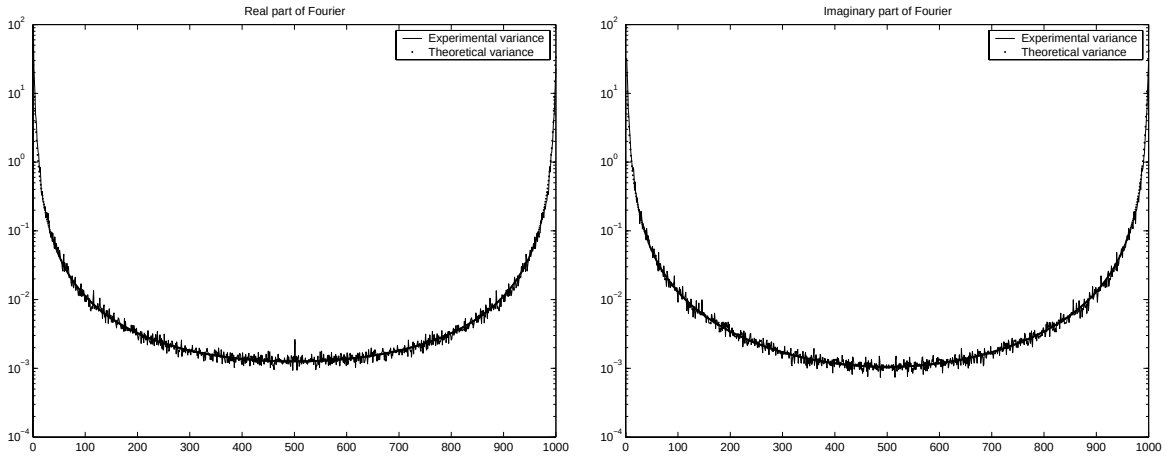
[27] Patrick Billingsley, *Probability and measure*, Wiley, 1995.

[28] S.M. Kay, *Fundamentals of Statistical Signal Processing: Detection Theory*, Prentice Hall, NJ, USA, 1998.

[29] Athanasios Papoulis, *Probability, random variables, and stochastic proccesses*, McGraw-hill, New York, 1991.

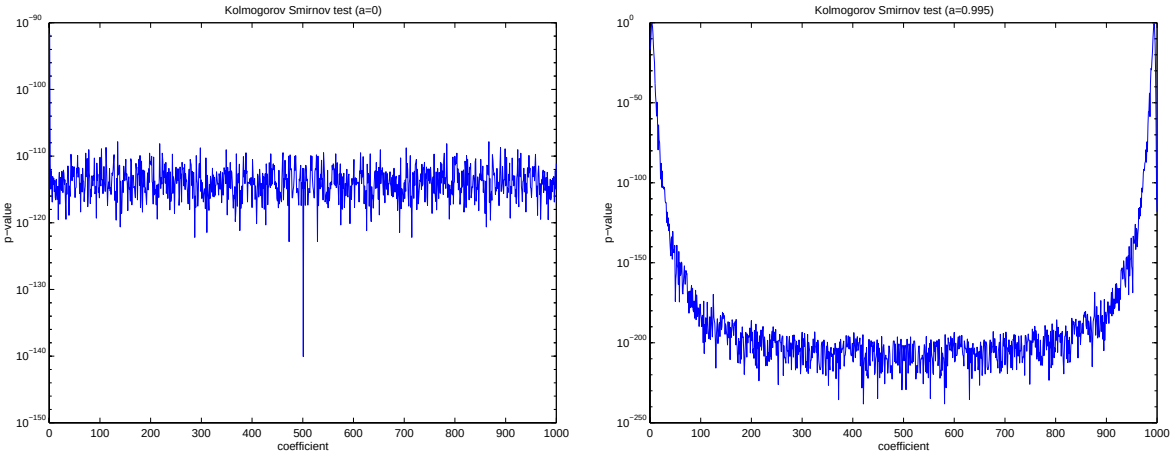
[30] Murray R. Spiegel, *Probability and Statistics*, McGraw-Hill, Inc., 1975.

[31] I.S.Gradshteyn and I.M.Ryzhik, *Table of Integrals, Series and Products*, Academic Press.



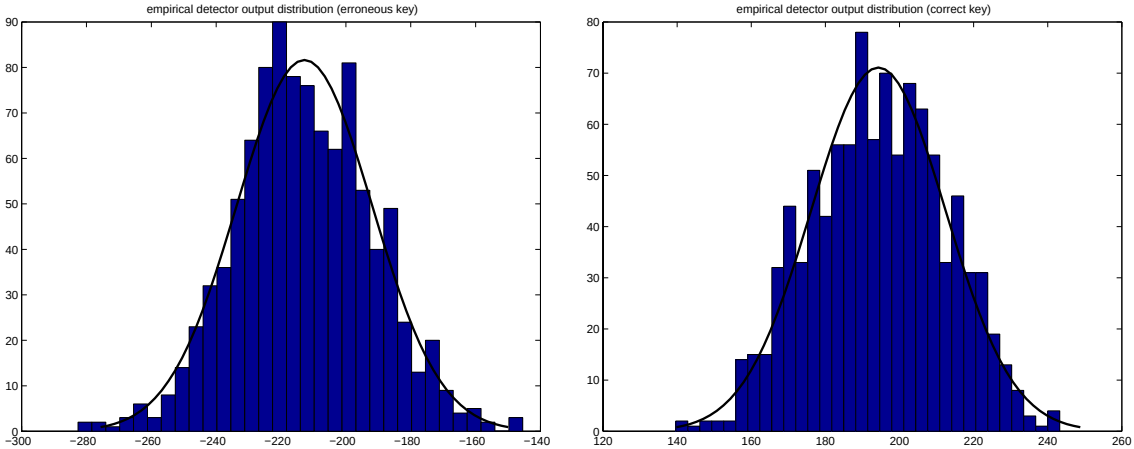
(a) (b)

Fig. 1. Theoretical and experimental variances of real (a) and imaginary (b) part of each Discrete Fourier coefficient of 100 signals of length 1000 having $a = 0.99$.



(a) (b)

Fig. 2. P-values (output of Kolmogorov-Smirnov test) for each coefficient of the real part of the Fourier transform of a signal (a) $a = 0$, (b) $a = 0.995$



(a) (b)

Fig. 3. Empirical detector output distribution (a) erroneous key, (b) correct key

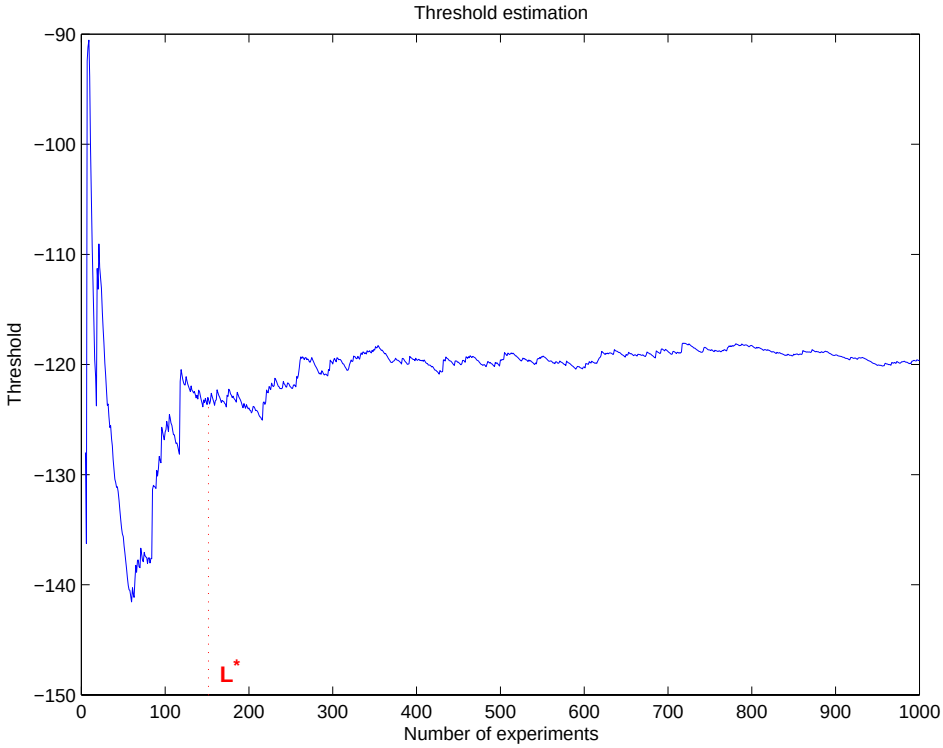


Fig. 4. Threshold estimation versus the number of experiments

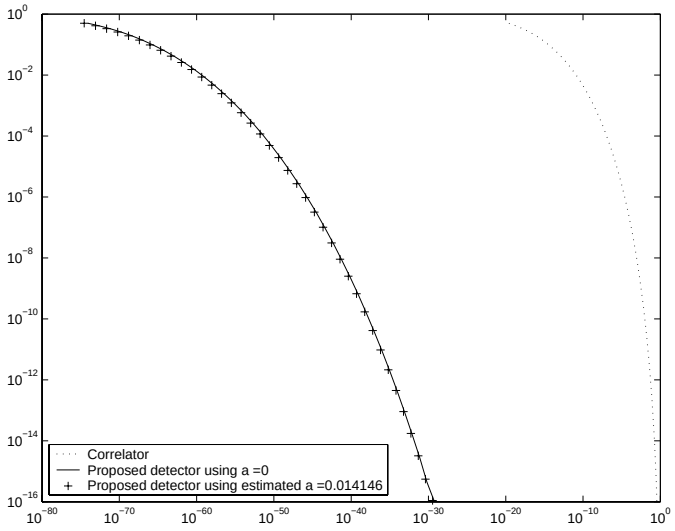


Fig. 5. ROC curves of correlator, the normalized correlator, the proposed detector by using the known parameter a and the proposed detector after estimating the parameter a. $a = 0$

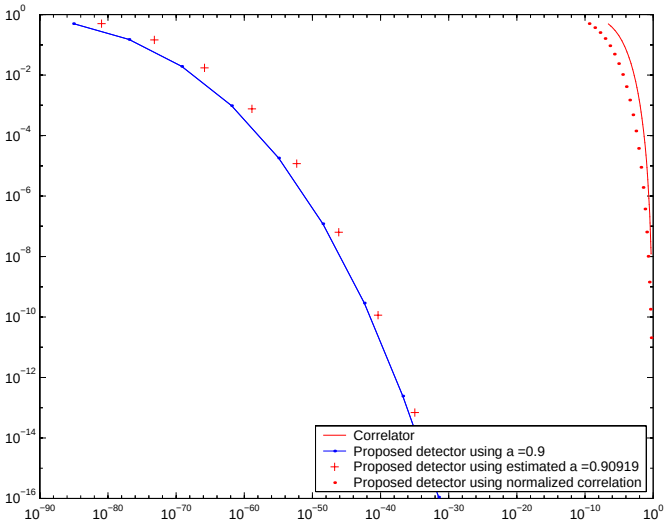


Fig. 6. ROC curves of correlator, the normalized correlator, the proposed detector by using the known parameter a and the proposed detector after estimating the parameter a. $a = 0.9$

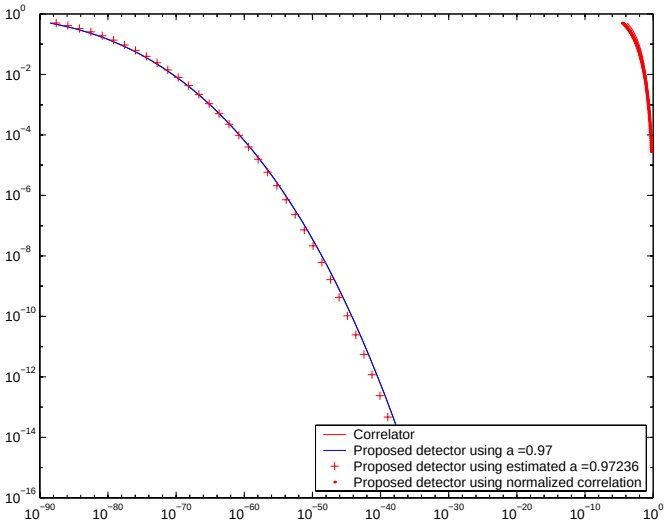


Fig. 7. ROC curves of correlator, the normalized correlator, the proposed detector by using the known parameter a and the proposed detector after estimating the parameter a. $a = 0.97$

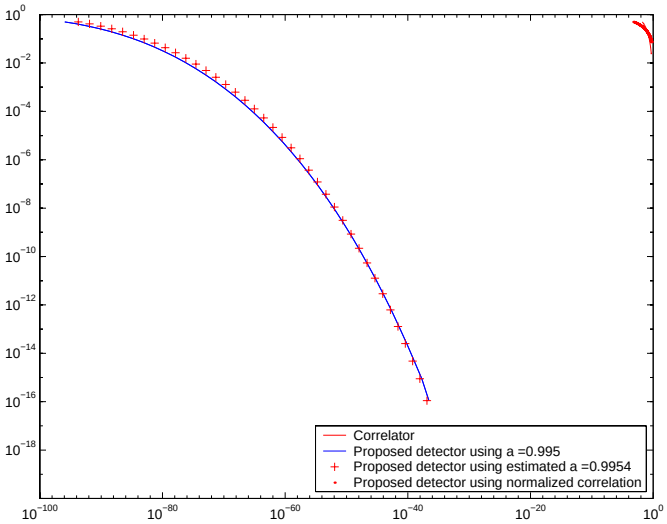


Fig. 8. ROC curves of correlator, the normalized correlator, the proposed detector by using the known parameter a and the proposed detector after estimating the parameter a. $a = 0.995$

List of Figures