# Optimum Detection of Multiplicative-Multibit Watermarking for Fingerprint Images

Khalil Zebbiche, Fouad Khelifi, and Ahmed Bouridane

School of Electronics, Electrical Engineering and Computer Science,
Queen's University Belfast
BT7 1NN Belfast, UK
{kzebbiche01,fkhelifi01,A.Bouridane}@qub.ac.uk

**Abstract.** Watermarking is an attractive technique which can be used to ensure the security and the integrity of fingerprint images. This paper addresses the problem of optimum detection of multibit, multiplicative watermarks embedded within Generalized Gaussian distribution features in Discrete Wavelet Transform of fingerprint images. The structure of the proposed detector has been derived using the maximum-likelihood approach and the Neyman-Pearson criterion. The parameters of the Generalized Gaussian distribution are directly estimated from the watermarked image, which makes the detector more suitable for real applications. The performance of the detector is tested by taking into account the different quality of fingerprint images and different attacks. The results obtained are very attractive and the watermark can be detected with low detection error. Also, the results reveal that the proposed detector is more suitable for fingerprint images with good visual quality.

**Keywords:** Fingerprint images, multibit watermarking, multiplicative rule, maximum-likelihood.

## 1 Introduction

Fingerprint-based authentication systems are the most advanced and accepted techniques of the biometric technologies. They have been used in law enforcement agencies and have been progressively automated over the last years. With the recent developments in fingerprint sensing, an increasing number of non-criminal applications are either using or actively considering using fingerprint-based identification. However, biometric-based systems, in general, and fingerprint-based systems, in particular, may risk several threats. Ratha et *al.* [1] describe eight basic sources of possible attacks on biometric systems. In addition Schneir [2] identifies many other types of abuses. Watermarking, which is one of the possible techniques that may be used, has been introduced to increase the security and the integrity of fingerprint data [3]-[7].

One of the most important stages in watermarking is the detection stage, which aims to decide whether a given watermark has been inserted within an image or not. This can be seen as a hypothesis testing in that the system has to decide the alternative hypothesis (the image is watermarked) and the null hypothesis (the image is not

S.-W. Lee and S.Z. Li (Eds.): ICB 2007, LNCS 4642, pp. 732–741, 2007.

watermarked). In binary hypothesis testing two kinds of errors can occur: accepting the alternative hypothesis, when the null hypothesis is correct and accepting the null hypothesis when the alternative hypothesis is true. The first error is often called false alarm error and the second error is usually called missed detection error.

The problem of watermarking detection has been investigated by many researchers; however, the most of these works consider the case of one-bit watermarking. The problem of assessing the presence of a multibit watermark is more difficult than the one-bit watermark because the information bits embedded are unknown for the detector. Hernandez et *al*. [8] derived an optimum detection strategy for additive watermarking rule, which cannot be used when another embedding rule is used. Barni et *al*. [9] proposed a structure of an optimum multibit detector for multiplicative watermarks embedded in Weibull distribution features.

In this paper, we propose an optimum detector of a multibit, multiplicative watermark embedded in the DWT coefficients of fingerprint images. The structure of the proposed detector is derived using a maximum-likelihood (ML) method based on Bayes' decision theory, whereby the decision threshold is obtained using the Neyman-Pearson criterion. A Generalized Gaussian Probability Density Function (PDF) is used to model the statistical behavior of the coefficients. The performance of the proposed decoder is examined through a number of experiments using real fingerprint images with different quality.

The rest of the paper is organized as follows: Section 2 shows how the watermark sequence is hidden into the DWT coefficients. Section 3 explains the derivation of the decision rule based on ML method while the derivation of the decision threshold is presented is Section 4. The experimental results are provided in Section 5. The conclusion is presented in Section 6.

## 2 Embedding Stage

The watermark is embedded into the DWT subbands coefficients. Let $b= \{b_1 \ldots b_{Nb}\}$ be the information bit sequence to be hidden (assuming value +1 for bit 1 and -1 for bit 0) and $m= \{m_1 m_2 \ldots m_{Nb}\}$ a pseudo-random set uniformly distributed in [-1, 1], which is generated using a secret key $K$. The information bits $b$ are hidden as follows: (i) the DWT subband coefficients used to carry the watermark are partitioned into $N_b$ non-overlapping blocks $\{B_i: 1 \le i \le N_b\}$. (ii) the watermark sequence $m$ is split into $N_b$ non-overlap chunks $\{M_i: 1 \le i \le N_b\}$ so that, each block $B_k$ and each chunk $M_k$ will be used to carry one in information bit. (iii) each chunk $M_k$ is multiplied by +1 or -1 according to the information bit $b_k$ to get an amplitude-modulated watermark. Finally, the watermark is embedded using the multiplicative rule, given by:

$$y_{B_k} = (1 + \gamma M_k b_k) x_{B_k} \tag{1}$$

where $x_{B_k} = \{x_{1B_k} x_{2B_k} \cdots x_{NB_k}\}$ and $y_{B_k} = \{y_{1B_k} y_{2B_k} \cdots y_{NB_k}\}$ are the DWT coefficients of an original image and the associated watermarked image belonging to the block $B_k$,

respectively. $\gamma$ is a positive scalar value used to control the strength of the watermark. The larger the strength, the more robust is the watermark but the visual quality of the image may be affected. So, it is important to set $\gamma$ to a value which maximizes the robustness while keeping the visual quality unaltered.

## 3 Maximum-Likelihood Detection

Since the exact information bit sequence is unknown for the detector for blind watermarking, multibit detection is more difficult than the one-bit case. However, an optimum detector for multibit watermark can be derived following the same approach for the one-bit watermark described in [10], [11]. The watermark is detected using ML based on Bayes' decision theory, whereby the decision threshold is derived using the Neyman-Pearson criterion which aim to minimize the missed detection probability for a fixed false alarm rate. According to this approach, the problem is formulated as a statistical hypothesis testing. Two hypotheses can be established as follows:

$H_0$: Coefficients are marked by a spreading sequence $m$, modulated by one of the $2^{Nb}$ possible bit sequence $b$.
$H_1$: Coefficients are marked with another possible sequence $m'$, including the null sequence, where $m' \neq m$.

The likelihood ratio, denoted by $l(y)$, is defined as:

$$l(y) = f_Y(y|m) / f_Y(y|m'). \tag{2}$$

where $f_Y(y|m)$ and $f_Y(y|m')$ represent the PDF of $y$ conditioned to the presence of the sequence $m$ and $m'$, respectively. In fact, it has been proved in [10] that for reasonably small value of the strength γ, the PDF of the coefficients $y$ conditioned to the event $m'$ can be approximated by the PDF of $y$ conditioned to the presence of the null sequence, $f_Y(y|0)$. The likelihood ration $l(y)$ becomes:

$$l(y) = f_Y(y|m) / f_Y(y|0). \tag{3}$$

Assuming that the information bits $b$ and the coefficients in $m$ are independent of each other, as well as the DWT coefficients used to carry the watermark. The PDF $f_Y(y|m)$ is obtained by integrating out the $2^{Nb}$ possible bit sequences.

$$\begin{aligned} f_Y(y|m) &= \prod_{k=1}^{N_b} f_Y(y_k|m_k) \\ &= \prod_{k=1}^{N_b} f_Y(y_k|m_k, -1)\, p(b_k = -1) + f_Y(y_k|m_k, +1)\, p(b_k = +1). \end{aligned} \tag{4}$$

By assuming that $p(b_k = -1) = p(b_k = +1) = 1/2$, equation (4) can be written as follows:

$$l(y)=\frac{\prod_{k=1}^{N_b}\frac{1}{2}\left[\prod_{i\in B_k}\frac{1}{1-\gamma m_{ki}}f_X\left(\frac{y_{ki}}{1-\gamma m_{ki}}\right)+\prod_{i\in B_k}\frac{1}{1+\gamma m_{ki}}f_X\left(\frac{y_{ki}}{1+\gamma m_{ki}}\right)\right]}{\prod_{k=1}^{N_b}\left[\prod_{i\in B_k}f_X\left(y_{ki}\right)\right]} \tag{5}$$

Further simplification can be made by taking the natural logarithm of the likelihood ratio, thus the decision rule can be expressed by

$$\begin{aligned}z(y)=\sum_{k=1}^{N_b}\Bigg\{-\ln(2)+\ln\Bigg[&\prod_{i\in B_k}\left(\frac{1}{1-\gamma m_{ki}}\right)f_X\left(\frac{y_{ki}}{1-\gamma m_{ki}}\right)-f_X\left(y_{ki}\right)\\&+\prod_{i\in B_k}\left(\frac{1}{1+\gamma m_{ki}}\right)f_X\left(\frac{y_{ki}}{1+\gamma m_{ki}}\right)-f_X\left(y_{ki}\right)\Bigg]\Bigg\}\end{aligned} \tag{6}$$

For an optimum behavior of the ML detector, it is necessary to describe the PDF of the DWT coefficients of the original image. An initial investigation using various distributions such as Laplacian, Gaussian and Generalized Gaussian has found that the Generalized Gaussian PDF is the most suitable distribution that can reliably model the DWT coefficients of the fingerprint images. It has been found that the Generalized Gaussian can also be used to model the coefficients for each block $B_k$. The central Generalized Gaussian PDF is defined as:

$$f_X(x_i;\alpha,\beta)=\left(\beta\Big/2\alpha\Gamma\left(1\Big/\beta\right)\right)\exp\left(-\left(|x_i|/\alpha\right)^{\beta}\right) \tag{7}$$

where $\Gamma()$ is the Gamma function, i.e., $\Gamma(z)=\int e^{-t}t^{z-1}dt$, z>0. The parameter $\alpha$ is referred to as scale parameter and models the width of the PDF peak (standard deviation) and $\beta$ is called the shape parameter and it is inversely proportional to the decreasing rate of the peak. Note that $\beta=1$ yields the Laplacian distribution and $\beta=2$ yields the Gaussian one. The parameter $\alpha$ and $\beta$ are estimated as described in [12].

Inserting (7) in (6), the decision rule for the Generalized Gaussian model is expressed by:

$$\begin{aligned}z(y)=\sum_{k=1}^{N_b}\Bigg\{-\ln(2)+\ln\Bigg[&\prod_{i\in B_k}\left(\frac{1}{1-\gamma m_{ki}}\right)\exp\left[\left(\frac{|y_{ki}|}{\alpha_{B_k}}\right)^{\beta_{B_k}}\left[1-\left|\frac{1}{1-\gamma m_{ki}}\right|^{\beta_{B_k}}\right]\right]\\&+\prod_{i\in B_k}\left(\frac{1}{1+\gamma m_{ki}}\right)\exp\left[\left(\frac{|y_{ki}|}{\alpha_{B_k}}\right)^{\beta_{B_k}}\left[1-\left|\frac{1}{1+\gamma m_{ki}}\right|^{\beta_{B_k}}\right]\right]\Bigg]\Bigg\}\end{aligned} \tag{8}$$

The decision rule reveals that an image is watermarked by the sequence $m$ ($H_0$ is accepted) only if $z(y)$ exceeds a threshold $\lambda$.

## 4 Decision Threshold

The Neyman-Pearson criterion is used in this work to obtain the threshold $\lambda$ in such a way that the missed detection probability is minimised, subject to a fixed false alarm probability $P^*_{FA}$. Fixing the value of $P^*_{FA}$, the threshold $\lambda$ can be obtained using the relation:

$$P^*_{FA} = P\left(z(y) > \lambda \middle| H_1\right) = \int_{\lambda}^{+\infty} f_z\left(z(y)\right) dz \tag{9}$$

where $f_z(z(y))$ is the PDF of $z$ conditioned to the event $H_1$. The problem now is to derive a good estimate of $f_z(z(y))$. One idea is to use Monte Carlo simulations to estimate the false alarm probability for different values of $\lambda$ and then choose the threshold $\lambda$ which leads to the desired false alarm. However, this approach is very computationally intensive, especially when Generalized Gaussian PDF is used to model the coefficients because the parameters $\beta$ and $\alpha$ are calculated numerically. Another simpler solution may be used to derive the threshold $\lambda$, by relying on the central limit theorem and assuming that the PDF of $z(y)$ can be assumed Gaussian with mean $\mu_z = E[z(y)]$ and $\delta_z^2 = V[z(y)]$ [9]. Equation (9) can be written as:

$$P^*_{FA} = \frac{1}{2} erfc\left(\frac{\lambda - \mu_z}{\sqrt{2\delta_z^2}}\right) \tag{10}$$

where *erfc*()is the complementary error function, so:

$$\lambda = erfc^{-1}\left(2P^*_{FA}\right)\sqrt{2\delta_z^2} + \mu_z . \tag{11}$$

The mean $\mu_z$ and the variance $\delta_z^2$ are estimated numerically by evaluating $z(y)$ for $n$ unreal sequences $\{ m_i : m_i \in [-1, 1]; 1 \le i \le n \}$, so that

$$\hat{\mu}_z = \frac{1}{n}\sum_{i=1}^{n} z_i \tag{12}$$

and

$$\hat{\delta}_z^2 = \frac{1}{n-1}\sum_{i=1}^{n}\left(z_i - \hat{\mu}_z\right)^2 \tag{13}$$

where $z_i$ represents the log likelihood ratio corresponding to the sequence $m_i$ and $n$ is the number of the fake sequences used to evaluate $z$. the selection of $n$ involves a trade-off between computational complexity and accuracy of results. The higher the $n$, the better the estimates of $\mu_z$ and $\delta_z^2$ but the higher computational complexity is and the less used in real applications, and inversely.

## 5 Experimental Results

The experiments were carried out using real fingerprint images of size 448×478 with different quality chosen from 'Fingerprint Verification Competition' (Db3_a,FVC

2000)[13] . Each image is transformed by DWT using Daubechies wavelet at the 3rd level to obtain low resolution subband ($LL_3$), and high resolution horizontal ($HL_3$), vertical ($LH_3$) and diagonal ($HH_3$) subbands. For reasons of imperceptibility and robustness, the watermark is embedded in the $HL_3$, $LH_3$, $HH_3$ subbands. Each subband is partitioned into blocks of size 16×16 (256 coefficients/block). A blind detection is used so that the parameters $\alpha$ and $\beta$ of each block used are directly estimated from the DWT coefficients of the watermarked image because it was assumed that the watermarked image is close to the original one (strength $\gamma$<<1). For all experiments, we choose 0.20 for $\gamma$ and $10^{-7}$ for $P_{FA}$.

Image 20_2

Image 22_7

Image 42_1

Image 44_6

**Fig. 1.** Test images

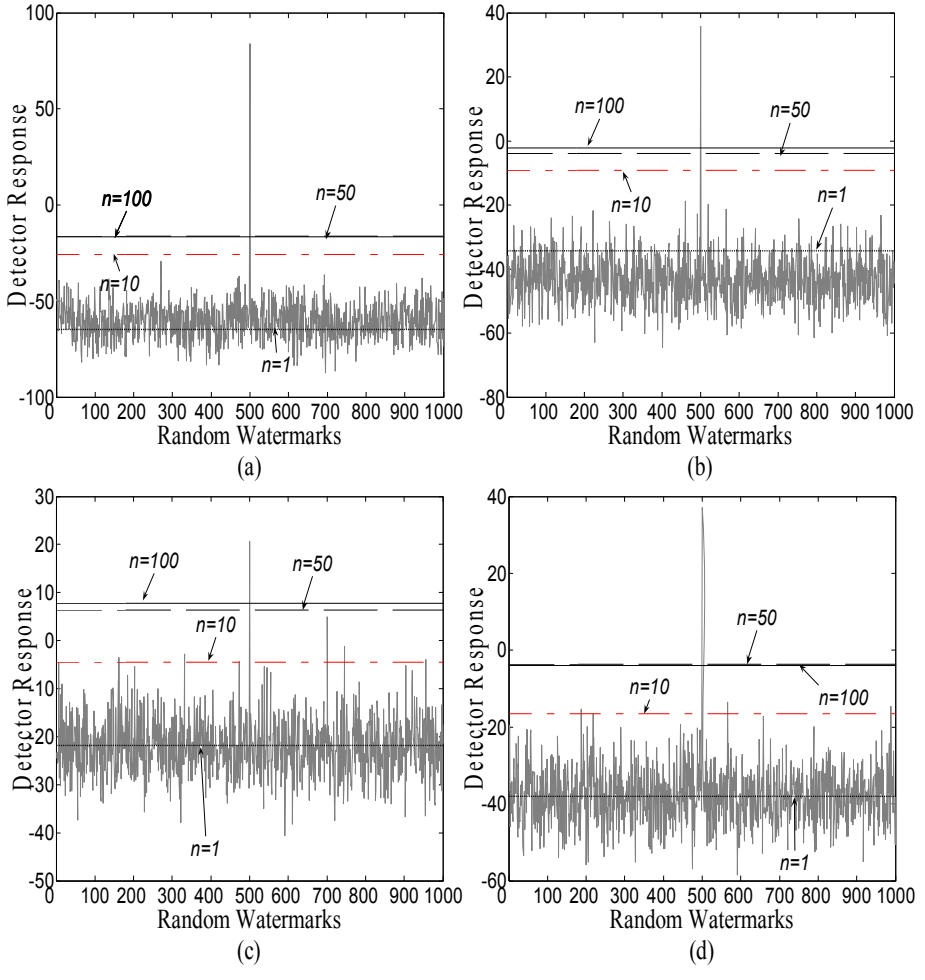


**Fig. 2.** Response of the watermark detector with different thresholds calculated with n=1, 10, 50, 100. (a) Image 20_2, (b) Image 22_7, (c) Image 42_1, (d) Image 44_6. γ=0.20 and $P_{FA}=10^{-7}$.

The first experiment is to determine the optimal value of *n*, necessary to derive the threshold λ with low complexity. To do so, the threshold λ is computed with different values of *n* (*n*=1, 10, 50, 100) and using fingerprint images of Fig. 1. We have also computed the responses of the detector to 1000 random watermarks where only one watermark among them is actually embedded. The results are plotted in Fig. 2.

The results obtained show that the different thresholds get closer when *n* increases and, in general, there is a slight difference between the threshold obtained with *n*=50 and *n*=100. Thus, n=50 yields a good threshold with a reasonable computational complexity. Further, the Fig. 2 shows that the correct response is much higher than those responses of the fake watermarks.

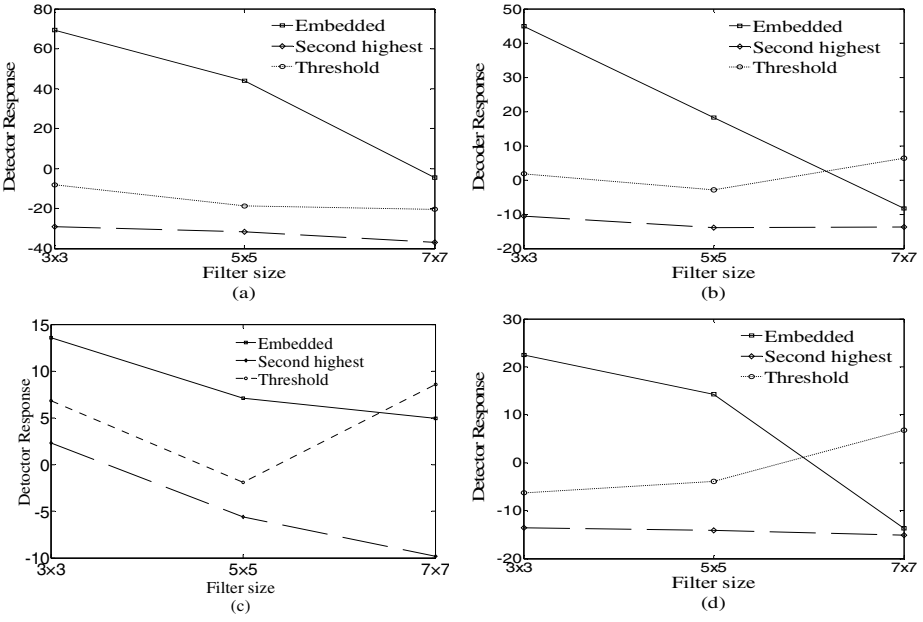


**Fig. 3.** Robustness against image filtering (mean filtering). Results refer to: (a) Image 20_2, (b) Image 22_7, (c) Image 42_1, (d) Image 44_6. with: $\gamma$=0.20, $n$=50 and $P_{FA}=10^{-7}$.

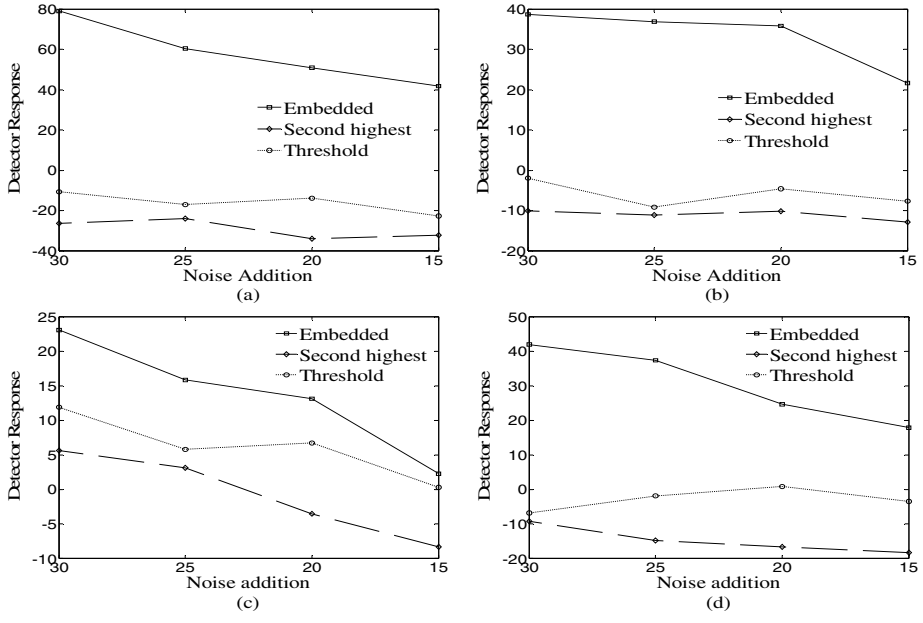


**Fig. 4.** Robustness against Gaussian noise addition. Results refer to: (a) Image 20_2, (b) Image 22_7, (c) Image 42_1, (d) Image 44_6. with: $\gamma$=0.20, $n$=50 and $P_{FA}=10^{-7}$.

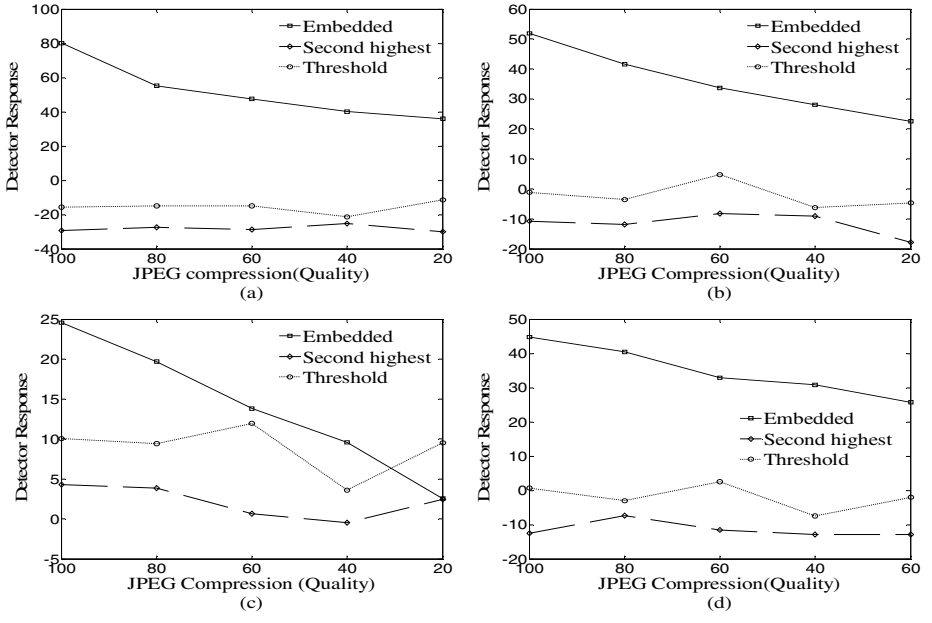


**Fig. 5.** Robustness against JPEG compression. Results refer to: (a) Image 20_2, (b) Image 22_7, (c) Image 42_1, (d) Image 44_6. with: $\gamma$=0.20, $n$=50 and $P_{FA}=10^{-7}$.

With $n$=50, we have also evaluated the performance of the detector against attacks such as mean filtering, image compression (JPEG) and White Gaussian Noise addition. Each attack has been applied several times with different strength i.e. increasing the size of the mean filter, decreasing the value of SNR for the Gaussian noise and decreasing the quality for JPEG compression. The results obtained are reported in Figs. 2, 3, 4. For each attack the response of the detector for 1000 randomly generated watermarks, including the one actually embedded within the image, has been measured. The response relative to the true watermark and the highest response among those corresponding to the other watermarks are plotted along with the threshold. In this way, both false alarm error and missed detection error are taken into account. The results obtained after applying mean filtering to the watermarked images are presented in Fig. 3. While, Fig. 4 shows the effect of the additive white Gaussian noise on both the detection response and the threshold. Fig. 5. provides the results for JPEG Compression. The results obtained clearly reveal that the proposed detector provides attractive results. For all attacks, the false alarm error does not occur while the missed detection error is obtained in few cases, especially for the mean filtering when the size of the filter is superior to 5.

## 6 Conclusion

In this paper, an optimum detector, based on the ML approach, for fingerprint image watermarking in the DWT domain has been proposed. The Generalized Gaussian

PDF has been used to model the statistical behavior of the DWT coefficients. The experiments reveals that the proposed detector provides very attractive results and the detecting error probability is very low, even in the presence of attacks. Also, the results confirm that the Generalized Gaussian is the most suitable distribution that can reliably model the DWT coefficients of fingerprint images. Further more, the quality of fingerprint images have an influence on the performance of the detector; we notice that the detector provides the best results for the images of good quality, where the ridges are very clear and represents the major part of the image.

## References

1. Ratha, N.K., Connell, J.H., Bolle, R.M.: Enhancing Security and Privacy in Biometrics-based Authentication systems. Proc. IBM Systems Journal 40 (2001)
2. Schneier, B.: The Uses and Abuses of Biometrics. Comm. ACM 42, 136 (1999)
3. Pankanti, S., Yeung, M.M.: Verification Watermarks on Fingerprint Recognition and Retreival. In: Proc. SPIE EI, San Jose, CA, vol. 3657, pp. 66–78 (1999)
4. Ratha, N.K., Connell, J.H., Bolle, R.M.: Secure Data Hiding in Wavelet Compressed Fingerprint Images. In: Proc. ACM Multimedia 2000 Workshops, Los Angeles, CA, pp. 127–130. ACM Press, New York (2000)
5. Uludag, U., Gunsel, B., Ballan, M.: A Spatial Method for Watermarking of Fingerprint Images. In: Proc. First Intl. Workshop on Pattern Recognition in Information Systems, Setúbal, Portugal, pp. 26–33 (2001)
6. Jain, A.K., Uludag, U.: Hiding Biometric Data. In: Proc. IEEE, vol. 25. IEEE Computer Society Press, Los Alamitos (2003)
7. Zebbiche, K., Ghouti, L., Khelifi, F., Bouridane, A.: Protecting Fingerprint Data using Watermarking. In: Proc. First AHS Conf., Istanbul, Turkey, pp. 451–456 (2006)
8. Hernandez, J.R., Amado, M., Perez-Gonzales, F.: DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and New Structure. IEEE Trans. Image Processing 9, 55–68 (2000)
9. Barni, M., Bartolini, F., De Rosa, A., Piva, A.: Optimum Decoding and Detecting of Multiplicative Watermarks. IEEE Trans. Signal Processing 51, 1118–1123 (2003)
10. Barni, M., Bartolini, F., De Rosa, A., Piva, A.: A New Decoder for the optimum recovery of nonadditive Watermarks. IEEE Trans. Image Processing 10, 357–372 (2001)
11. NG, T.M., Garg, H.K.: Wavelet Domain Watermarking using Maximum-Likelihood Detection. In: Proc. SPIE Conf. Security, Steganographie, Watermarking Multimedia, San Jose, CA, vol. 5306 (2004)
12. Do, M.N., Vetterli, M.: Wavelet-based Texture Retrieval using Generalized Gaussian and Kullback-Leibler. IEEE Trans. Image Processing 11, 146–158 (2002)
13. Fingerprint Verification Competition: http://bias.csr.unibo.it/fvc2000/download.asp