Hindawi Publishing Corporation
International Journal of Digital Multimedia Broadcasting
Volume 2008, Article ID 492942, 13 pages
doi:10.1155/2008/492942

Research Article

Region-Based Watermarking of Biometric Images: Case Study in Fingerprint Images

K. Zebbiche and F. Khelifi

School of Electronics, Electrical Engineering and Computer Science, Queen's University of Belfast, Belfast BT7 1NN, UK

Correspondence should be addressed to K. Zebbiche, kzebbiche01@qub.ac.uk

Received 1 March 2008; Accepted 27 June 2008

Recommended by Harald Kosch

In this paper, a novel scheme to watermark biometric images is proposed. It exploits the fact that biometric images, normally, have one *region of interest*, which represents the relevant part of information processable by most of the biometric-based identification/authentication systems. This proposed scheme consists of embedding the watermark into the region of interest only; thus, preserving the hidden data from the segmentation process that removes the useless background and keeps the region of interest unaltered; a process which can be used by an attacker as a cropping attack. Also, it provides more robustness and better imperceptibility of the embedded watermark. The proposed scheme is introduced into the optimum watermark detection in order to improve its performance. It is applied to fingerprint images, one of the most widely used and studied biometric data. The watermarking is assessed in two well-known transform domains: the discrete wavelet transform (DWT) and the discrete Fourier transform (DFT). The results obtained are very attractive and clearly show significant improvements when compared to the standard technique, which operates on the whole image. The results also reveal that the segmentation (cropping) attack does not affect the performance of the proposed technique, which also shows more robustness against other common attacks.

1. INTRODUCTION

Biometric-based systems that use physiological characteristics and/or behavioral traits offer a good alternative to traditional systems such as token-based or knowledge-based systems. These systems are more reliable and more user friendly. However, there are many issues that need more attention, especially the security aspect of both biometric system and biometric data. Several researchers show the existence of many threats and attacks that may affect the security and the integrity of biometric-based systems [1–4]. The problems that may arise from the attacks on such systems are raising concerns as more and more biometric systems are deployed [5]. Some techniques such as cryptography and watermarking have been introduced to thwart some of these attacks. Watermarking techniques are gaining more interest by providing promising results [6–8]. For example, watermarking of fingerprint images can be used to secure central databases from which fingerprint images are transmitted on request to intelligence agencies in order to use them for identification purposes (see Figure 1).

In the literature, watermarking has been introduced and shown to be satisfying the need for the protection of digital data. It can be used for many security purposes such as copyright protection, fingerprinting, copy protection, data authentication, and so forth [9]. Depending on the application, the watermarking schemes can be cast in two classes. In the first class, often known as multibit watermarking, a specific data, such as ID or track number, is embedded into the host data. In this case, the embedded watermark communicates a multibit message which must be extracted accurately at the decoding side [10, 11]. In the second class, it is not known whether a candidate watermark is embedded in the input data. The task here is therefore to verify the presence of the watermark, usually referred to as watermark detection [12, 13].

In these applications, the basic requirement is that the watermark should remain in the host data, even if its quality is degraded, intentionally or unintentionally. Examples of unintentional degradations are applications involving storage or data transmission where lossy compression is used; also filtering, resampling, digital-analog (D/A), and

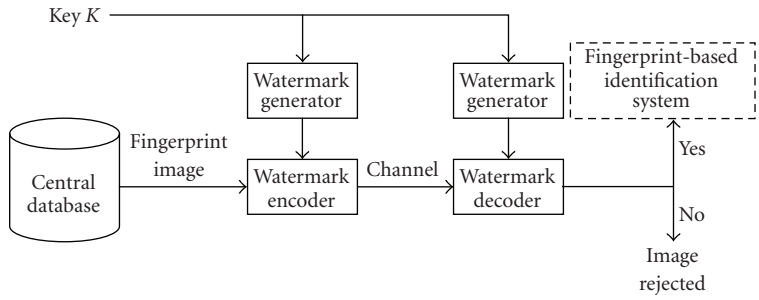


Figure 1: Block diagram of a watermarking application for fingerprint images.

analog-digital (A/D) conversion may affect the quality of the image. The host data can also be intentionally attacked in order to remove the watermark by using malicious data processing techniques such as noise addition, cropping, rotation, and translation.

The cropping technique, which consists of removing a portion of the image, remains one of the toughest attacks to deal with. Indeed, the attacker might apply it to take out parts of the image which are useless; hence, a portion of the watermark embedded within these regions is easily removable. Unfortunately, most of the watermarking algorithms are not robust enough to such an attack. Also, the watermark algorithms that make use of the human visual systems (HVSs) characteristics intend to maximize the inserted watermark, especially, in the texture areas but these algorithms do not make the difference between the useful textures and the useless noise. In order to overcome this problem, the watermark should be inserted into the most relevant part(s) of the image, that is, *region of interest* (ROI). However, this is difficult to apply to natural images since the ROI of such images is user-dependent or just undefined.

Several biometric-based systems, such as fingerprint, face, iris, or hand, use images as input data. A common characteristic of these images is that they have only one ROI, constituting the part processable by the identification/authentication algorithms. The segmentation technique is usually used to extract the ROI. However, this technique, which is basically used as a preprocessing step, can be used by an attacker as a special case of cropping since it removes the background area (i.e., removes the part of the watermark embedded in this area) while keeping ROI unchanged. The motivation is that the idea of inserting the watermark into the ROI is applicable to biometric images whose ROI can be extracted.

In this work, we propose a new scheme to embed the watermark into the ROI of biometric images. This is motivated by the following: (i) securing the embedded watermark against the segmentation process and increasing the robustness of the watermark against other attacks such as filtering, noise because even the attacker knows that the watermark is embedded in this region, concentrating his attacks on that area degrades significantly its quality, hence, making it useless; (ii) providing more transparency to the embedded watermark since the human eye is less sensitive to changes in textured areas.

Region-based method proposed in this work can be viewed as a special case of personalization because the proposed algorithm is adaptive and only a portion of the data (i.e., ROI) is watermarked. The proposed scheme is applied on fingerprint images. Note that fingerprint-based systems are regarded as the most powerful and widely deployed biometric systems. To extract the ROI of such images, referred here to as *ridges area*, the segmentation technique proposed by Wu et al. [14] is modified in order to use adaptive thresholding. For sake of completeness, the watermark is embedded into the discrete wavelet transform (DWT) and discrete Fourier transform (DFT), where the DWT coefficients are statistically modeled by the generalized Gaussian distribution (GGD) and the DFT coefficients are modeled by the Weibull distribution. Experiments were carried out on test images from real-fingerprint database and the results obtained clearly show the performance introduced by the proposed scheme. Also, the robustness of inserting the watermark into the ROI is assessed in the presence of attacks such as wavelet scalar quantization (WSQ) compression, mean filtering and additive white Gaussian noise (AWGN).

The paper is organized as follows: the proposed watermarking scheme for biometric images is explained in Section 2. Application of the proposed scheme to fingerprint images is described in Section 3. Experiments were carried out in Section 4 to assess the impact of the proposed technique on the overall performance of the optimum detector. Finally, conclusions are drawn in Section 5.

2. PROPOSED WATERMARKING SCHEME FOR BIOMETRIC IMAGES

The proposed watermarking scheme is depicted by Figure 2. At the encoder side, we aim to insert the watermark into the ROI only and exclude the background area; therefore, the ROI is first extracted. The extraction techniques can be either block-wise or pixel-wise and usually provide a binary image, called *region mask*, where 1 indicates that the block (or pixel) belongs to the ROI and 0 indicates that the block (or pixel) belongs to the background area. Then, the region mask is divided into nonoverlapping blocks to obtain a *watermarking mask*; where each block is classified based on the number of 1 in it. If the number of 1 exceeds a given threshold, then the block is classified as ROI block, otherwise, it is a background

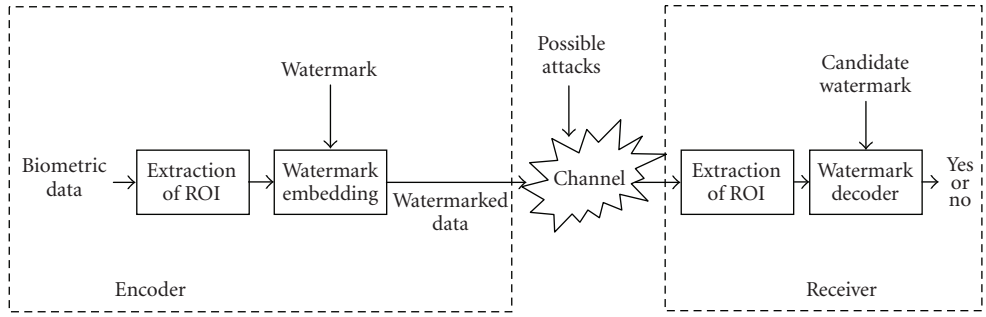


Figure 2: Proposed watermarking scheme for biometric data.

block. This watermarking mask is used to select the blocks that will hold the watermark.

It is worth noting that there are two issues to be taken into account when choosing the ROI extraction technique for watermarking purposes, which are as follows: (i) the robustness of the technique against possible attacks that may affect a watermarked image, that is, the ROI extraction technique must extract approximately the same ROI from the original and the watermarked images even after applying attacks; (ii) computational complexity. Indeed, the block-wise extraction scheme is less complex than the pixel-wise one. However, this comes at the cost of accuracy. From the view point of watermarking, pixel-wise extraction techniques are more powerful since they provide more accuracy of ROI at the detector side. This is obviously required in blind watermarking. The proposed watermarking scheme is equipped with an optimum watermark detector. In such a case, the false-alarm probability (P_{fa}) and the detection probability (P_{det}) are the natural performance measures.

3. APPLICATION TO FINGERPRINT IMAGES

The region-based method proposed in this paper can be viewed as a special case of personalization because the algorithm adaptively operates on a portion of the input data (i.e., ROI) as illustrated by Figure 3. As can be seen, the encoding system uses the ROI to insert the watermark and keeps the background image unchanged. The bigger the ROI, the larger the number of coefficients that can be used for watermarking. Once the watermark is embedded, the background area is used to reconstruct the watermarked image. At detection, the detector follows the same steps to extract the ROI and check the presence of the watermark. It is worth mentioning that the selected extraction method is first assessed on the original images by varying the attacks strength. This method should be robust enough to attacks that might alter the watermarked image. Although the watermarked image may undergo attacks that aim to remove the watermark, the visual quality should be kept useful so that the attacker can use it. We have carried out experiments on the original images to verify the efficiency of the extraction method against different attacks with various strengths controlled by a number of parameters such as compression ratio, noise variance, filtering window size.

3.1. Region of interest extraction

A fingerprint is a pattern of alternating convex skin called *ridges* and concave skin called *valleys* with a spiral-curve-like line shape. In fingerprint images, the ridges area is considered as the ROI and the noisy area around it and at the borders is the background area. In the literature, several methods have been proposed to extract the ROI from fingerprint images. These methods can be divided into two categories: block-wise and pixel-wise features classification. The algorithms that fall in the first category decompose the image into blocks. Then, some characterizing features, such as the local histogram of ridge orientation, gray-level variance, magnitude of the gradient, are calculated and based on these features, a classifier can be used to decide whether a block belongs to the ROI or to the background area. In the second category, pixel features are first extracted. This includes for example coherence, average gray level, variance and Gabor response, and then a simple classifier is chosen for classification. Such pixel-wise methods provide accurate results, but their computational complexity is higher than the commonly used block-wise methods.

In this work, Harris corner point features method [14] is adopted to extract the ridges area of fingerprint images. The Harris corner detector is based on the local autocorrelation function of a signal; where the local autocorrelation function measures the local changes of the signal with patches shifted by a small amount in different directions [15]. Wu et al. found in [14] that the strength of the Harris point in the ridges area is much higher than that of the background area. However, the authors used different thresholds, which are determined experimentally for each image. Also, they reported the existence of some noisy regions in the background area corresponding to high strength values, which cannot be eliminated even by using high threshold values and proposed to use a heuristic algorithm based on the corresponding Gabor response in order to discard these noisy regions.

To make this technique more flexible and practical, it has been modified by using the Otsu thresholding method [16] to adaptively determine adequate thresholds. Otsu method is based on maximizing the between-class variance to find the optimum threshold. This modification provides an excellent threshold for fingerprint images with different visual

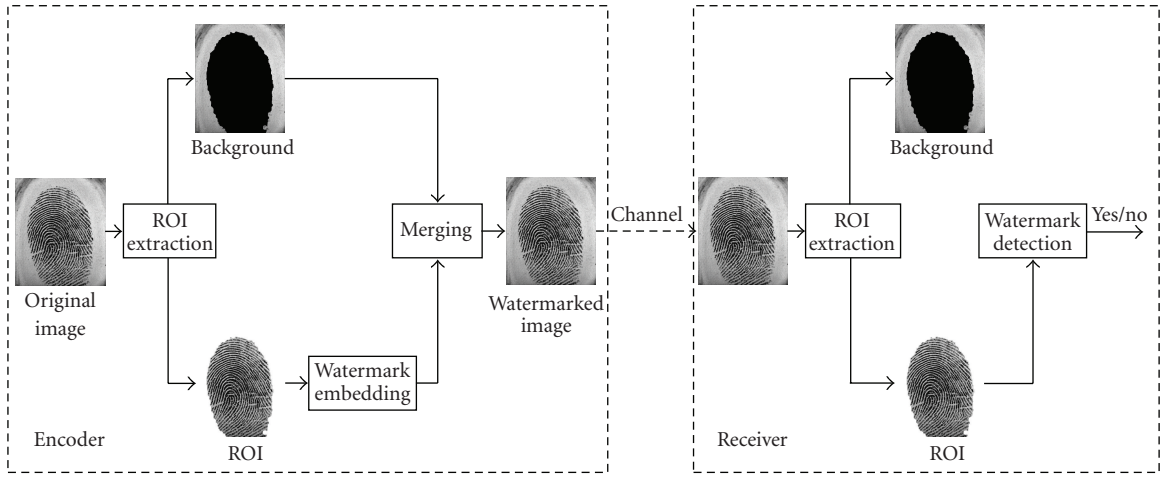


Figure 3: Personalized watermarking system applied to fingerprint images.

(a) (b) (c)

Figure 4: Example of fingerprint image: (a) original image, (b) region mask, (c) watermarking mask. The block size = 32.

qualities. To eliminate the noisy regions, some morphological methods are then applied, leading to excellent segmented images.

The Harris point is a pixel-wise method, the segmentation mask (Figure 4(b)) has the same size as the original image and it is partitioned to obtain the watermarking mask (Figure 4(c)). Note that in this paper, only blocks whose all pixels belong to the ridges area are taken into account, that is, 100% of the pixels belong to the ridges area for every selected block.

3.2. Watermark embedding

The watermark is embedded into the transform domain. In this paper, we consider two widely used transforms: the DWT and the DFT. These transforms can be applied to the entire image or in a block-wise manner. Also, the multiplicative rule is used to embed the watermark due to its advantages over the additive one, especially in exploiting the HVS characteristics. The watermark, denoted by $w = \{w_1, w_2, \ldots, w_N\}$, is a pseudorandom sequence uniformly distributed in $[-1, +1]$ and generated by using a secret key K. The embedding process is comprised of the steps described below.

(i) Extract the ROI for the input image I and obtain the region mask RM.

(ii) Determine the watermarking mask WM from the ROI by decomposing RM into nonoverlapping blocks of size $m \times m$.

(iii) Decompose the image I into nonoverlapping blocks B_{ij} of size $m \times m$ pixels and only the blocks that belong to the ROI are selected to carry the watermark, that is, if $\mathrm{WM}_{ij} = 1$ the corresponding block B_{ij} is selected; otherwise, it remains unchanged.

(iv) Transform the selected blocks using a transform, such as DWT and DFT, to obtain the original coefficients $x = \{x_1, x_2, \ldots, x_N\}$. The watermark is embedded into the original image using the multiplicative rule as follows:

$$y_i = (1 + \lambda w_i) x_i, \tag{1}$$

where $y = \{y_1, y_2, \ldots, y_N\}$ represents the watermarked coefficients and λ is the strength of the watermark.

3.3. Watermark detection

The goal of the optimum watermark detector is to verify whether or not there is a candidate watermark embedded in the received image, based on its statistical properties. This problem is usually formulated as a binary hypothesis test, in which, two hypotheses are used to represent the presence/absence of a given watermark within the host data. The two hypotheses can be established as follows:

H_0: the coefficients y are not watermarked by the candidate watermark w^*;

H_1: the coefficients y are watermarked by the candidate watermark w^*.

The decision rule for the binary test formulated above, denoted by $\Lambda(y)$, relies on maximum-likelihood method

based on Bayes' decision theory. The likelihood ratio can be written as

$$\Lambda(y) = \frac{f_y(y|H_1)}{f_y(y|H_0)}, \tag{2}$$

where $f_y(y|H_1)$ and $f_y(y|H_0)$ represent the probability distribution function (pdf) of vector y conditioned to the hypotheses H_1 and H_0, respectively. Following the same steps as described by Barni et al. in [12], the decision rule is defined as

$$l(y) = \sum_{i=1}^{N}\left[\ln\left(f_{x_i}\left(\frac{y_i}{1+\lambda w_i^*}\right)\right) - \ln(f_{x_i}(y_i))\right] \gtrless_{H_0}^{H_1} \eta', \tag{3}$$

where $l(y) = \ln(\Lambda(y))$. The decision rule reveals that H_1 is accepted (i.e., the coefficients y are marked by the sequence w^*) only if $l(y)$ exceeds the threshold η'. By employing the Neyman-Pearson criterion [17], the threshold is obtained in such a way that the detection probability P_{det} is maximized, subject to a fixed false-alarm probability P_{fa} [12]:

$$\eta' = \text{erfc}^{-1}(2P_{\text{fa}})\sqrt{2\sigma_0^2} + \mu_0, \tag{4}$$

where erfc$(\cdot)$ is the complementary error function, $\mu_0 = E[l(y)|H_0]$ and $\sigma_0^2 = V[l(y)|H_0]$ are the mean and the variance of $l(y)$ under hypothesis H_0, respectively.

3.3.1. Optimum watermark detector structure based on the GGD

To describe the probability characteristics of DWT coefficients, the GGD is widely used in the literature and some studies show that this distribution provides the closest approximation [18]. The GGD pdf of zero-mean is given by

$$f_X(x;\alpha,\beta) = \frac{\beta}{2\alpha\Gamma(1/\beta)}\exp\left(-\left(\frac{|x|}{\alpha}\right)^{\beta}\right), \tag{5}$$

where $\Gamma(\cdot)$ is the Gamma function, $\Gamma(z) = \int_0^{\infty} e^{-t}t^{z-1}dt$, $z > 0$. The parameter α is referred to as the scale parameter and it models the width of the pdf peak (standard deviation) and β is called the shape parameter and it is inversely proportional to the decreasing rate of the peak.

By substituting (5) in (3), the log-likelihood for the GGD is given by [19]

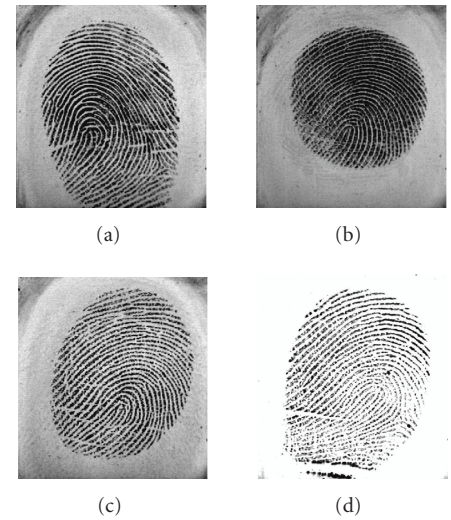
$$l(y) = \sum_{i=1}^{N}\left(\frac{|y_i|}{\alpha}\right)^{\beta}[1 - |1+\lambda w_i^*|^{-\beta}], \tag{6}$$

where α and β are the parameters of the GGD for the coefficients y.

The threshold η' can be obtained by using (4), where μ_0 and σ_0^2 are given by

$$\begin{aligned}\mu_0 &= \sum_{i=1}^{N}\frac{1}{\beta}[1 - |1+\lambda w_i^*|^{-\beta}],\\ \sigma_0^2 &= \sum_{i=1}^{N}\frac{1}{\beta}[1 - |1+\lambda w_i^*|^{-\beta}]^2.\end{aligned} \tag{7}$$

The parameters α and β can be estimated as described in [20].



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

Figure 5: Test images with different visual quality from DB3: (a) Image 22_6, (b) Image 88_1, (c) Image 46_2, and (d) Image 24_3.

3.3.2. Optimum detector structure based on the Weibull model

The DFT coefficients are widely modeled by the Weibull distribution in the literature [12, 21]. Its pdf is defined as

$$f_X(x;\alpha,\beta) = \frac{\beta}{\alpha}\left(\frac{x}{\alpha}\right)^{\beta-1}\exp\left[-\left(\frac{x}{\alpha}\right)^{\beta}\right], \quad x \geq 0, \tag{8}$$

where $\beta > 0$ represents the shape parameter and $\alpha > 0$ is the scale parameter of the distribution. The detector structure for the Weibull distribution is defined by Barni et al. [12] and given by

$$l(y) = \sum_{i=1}^{N} y_i^{\beta}\left(\frac{(1+\lambda w_i^*)^{\beta} - 1}{\alpha^{\beta}(1+\lambda w_i^*)^{\beta}}\right), \tag{9}$$

where α_i and β_i are the parameters of the Weibull model for the coefficients y.

Equation (4) is used to derive the threshold η' where the mean μ_0 and the variance σ_0^2 are defined as

$$\begin{aligned}\mu_0 &= \sum_{i=1}^{N}\left(\frac{(1+\lambda w_i^*)^{\beta} - 1}{(1+\lambda w_i^*)^{\beta}}\right),\\ \sigma_0^2 &= \sum_{i=1}^{N}\left(\frac{(1+\lambda w_i^*)^{\beta} - 1}{(1+\lambda w_i^*)^{\beta}}\right)^2.\end{aligned} \tag{10}$$

4. EXPERIMENTAL RESULTS

In order to efficiently measure the actual performance of proposed technique, experiments were carried out on real fingerprint images of size 448×478 taken from Fingerprint Verification Competition "FVC 2000, DB3" database [22]. These images have been chosen with respect to their different visual quality (Figure 5). The performance of the proposed technique, which embeds the watermark in the ridges area

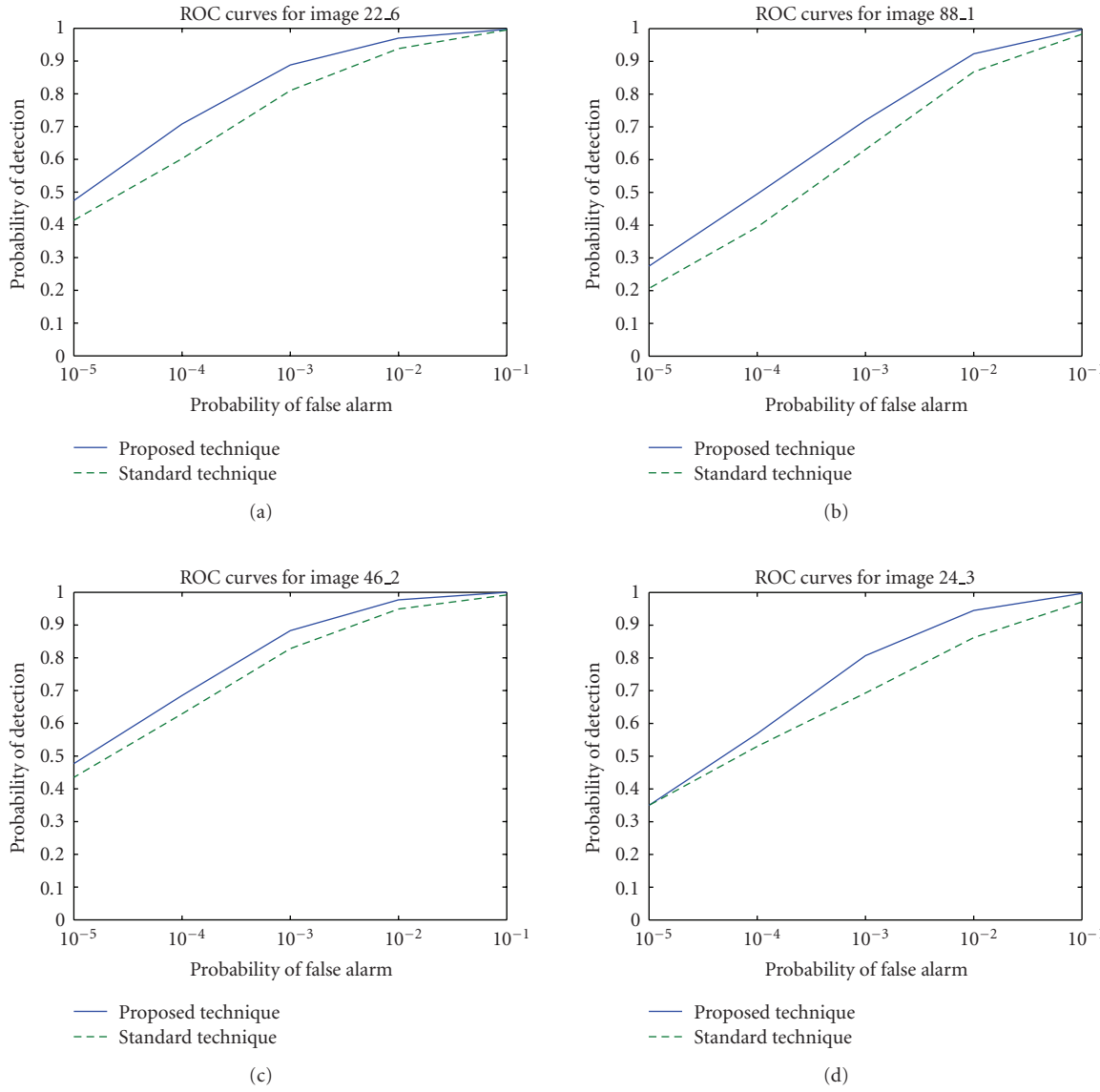


Figure 6: ROC curves of test images. Watermarking applied in the DWT domain. Strength $\lambda = 0.10$.

only, is compared against the standard technique which inserts the watermark into the whole image. In the DWT domain, Daubechies 9/7 wavelet is used. Note that such a wavelet has been adopted by the FBI as part of the wavelet scalar quantization (WSQ) compression standard for fingerprint images. The watermark is embedded in all coefficients in the third level subbands, except the approximation subband. An approach similar to that proposed in [12] is used to cast the watermark in the DFT domain, where the watermark is inserted into the magnitude of a set of full-frame coefficients. Blind detection is adopted for all experiments, that is, the statistical model parameters are directly estimated from the watermarked data. The receiver operating characteristics (ROCs) curves are used to assess the performance of both the proposed and the standard techniques. The ROC curves represent the variation of the detection probability (P_{det}) against the false-alarm probability (P_{fa}). Note that for our proposed technique, the number of coefficients to be watermarked (the length of the watermark sequence) is image dependent. The larger the ROI (i.e., ridges area), the higher the number of coefficients to be watermarked (the length of the watermark) and vice versa. For the size of the blocks m used to determine the watermarking mask, it has been set to 32 after extensive experiments held on many fingerprint images. This value allows the extraction of the ridges area even after applying severe attacks.

At the first stage, we investigate the performance of the proposed technique against the standard one without the presence of any attack. The probability of false alarm is varied in the range 10^{-5} to 10^{-1} and the value of the strength λ is fixed to value 0.10. The experimental ROC curves

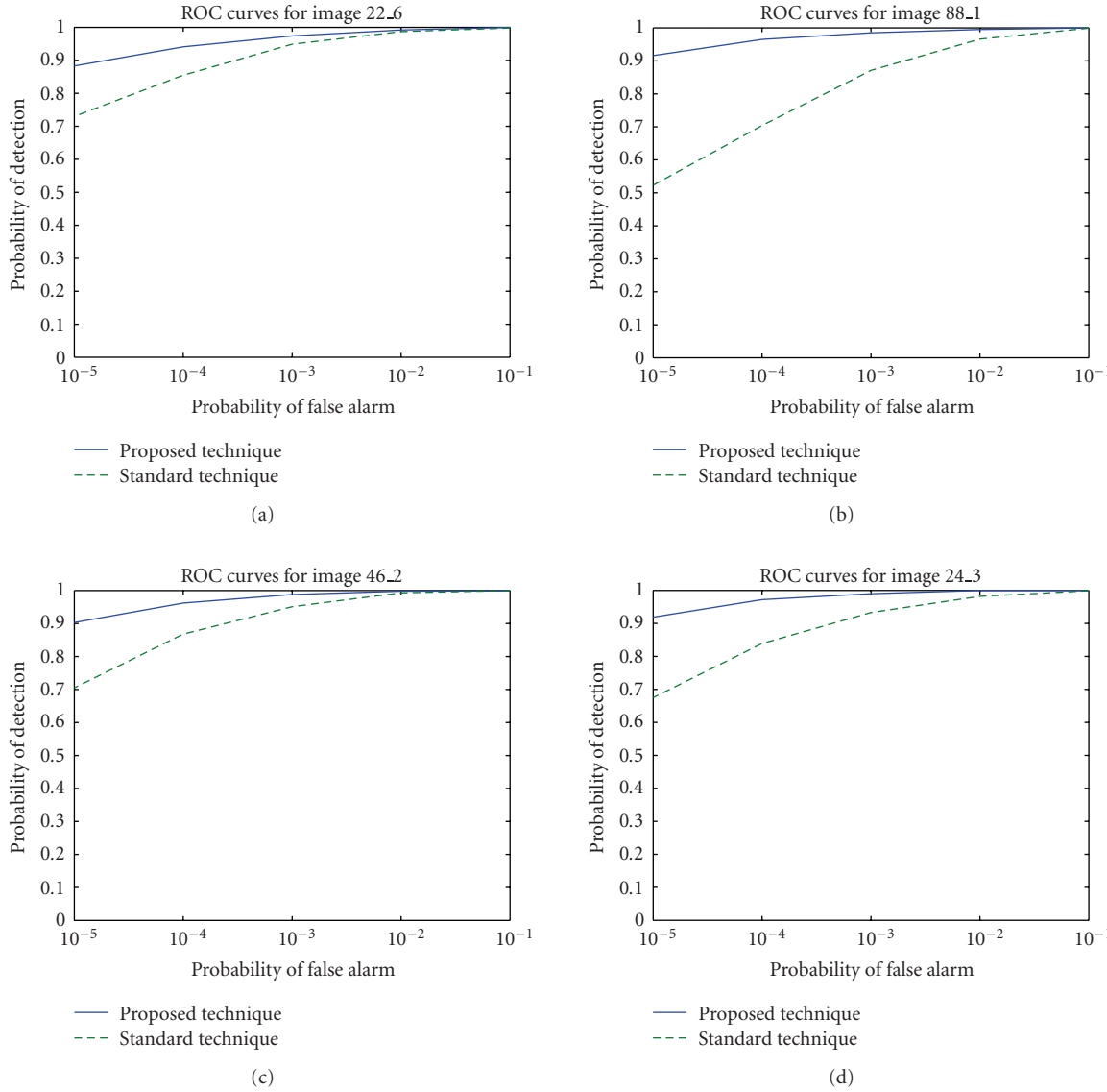


Figure 7: ROC curves of test images. Watermarking applied in the DFT domain. Strength $\lambda = 0.10$.

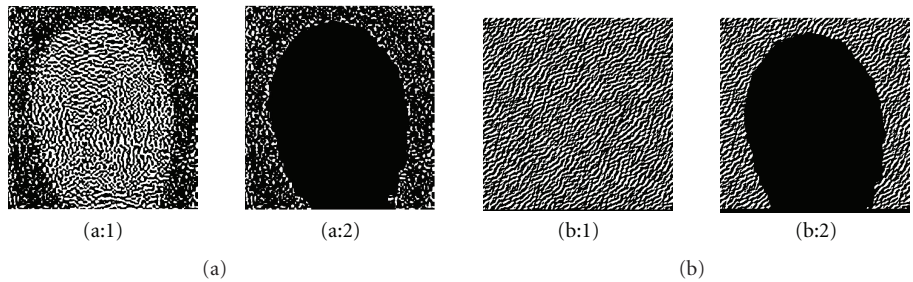


Figure 8: Standard watermarking of test image. Image 22_6: (a:1): difference image between original and watermarked images in the DWT domain; (a:2): difference image when removing ROI in the DWT domain; (b:1): difference image between original and watermarked images in the DFT domain; (b:2): difference image when removing ROI in the DFT domain.

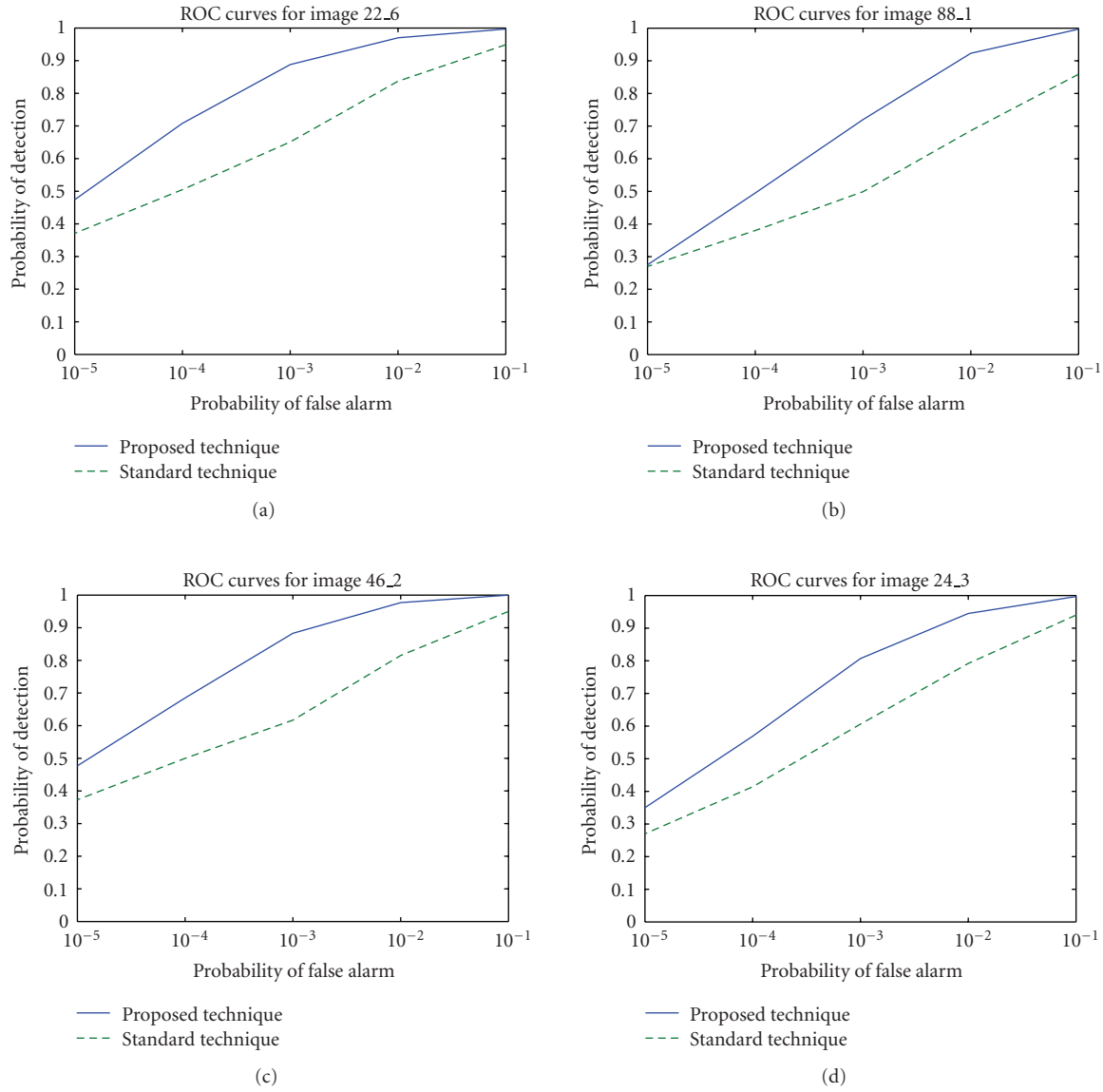


Figure 9: ROC curves of segmented, watermarked images. Watermarking applied in the DWT domain. Strength $\lambda = 0.10$.

are computed by measuring the performance of the actual watermark detection system by calculating the probability of detection from real-watermarked images. Experiments are then conducted by comparing the likelihood ratio with the corresponding threshold for each value of the false-alarm probability and for 1000 randomly generated watermark sequences. The results obtained for the DWT domain are plotted in Figure 6 and those obtained for the DFT domain are plotted in Figure 7.

As can be seen from Figures 6 and 7, the proposed technique outperforms the standard one even without applying any attack. This is justified by the fact that the transform coefficients are better suited to watermarking for the proposed technique since they correspond to a highly textured area (i.e., ridges area) only. These coefficients allow the embedding of strong watermarks.

As mentioned earlier, an attacker may use segmentation techniques on biometric images to remove a part of the watermark embedded within the background area without altering the ROI. To illustrate this, the spatial repartition of the watermark is plotted in Figure 8(a:1) for the DWT domain and in Figure 8(b:1) for the DFT domain in the case of a standard watermarking; it represents the difference between the watermarked image and the original one. The part of the watermark removed by the segmentation technique is plotted in Figure 8(a:2) for the DWT domain and in Figure 8(b:2) for the DFT domain. It represents the difference image without the ridges area. For the sake of illustration, only the results for one image is shown since the results for other images are very similar. As can be seen, an important part of the watermark is embedded into the background area, which can be removed easily by applying

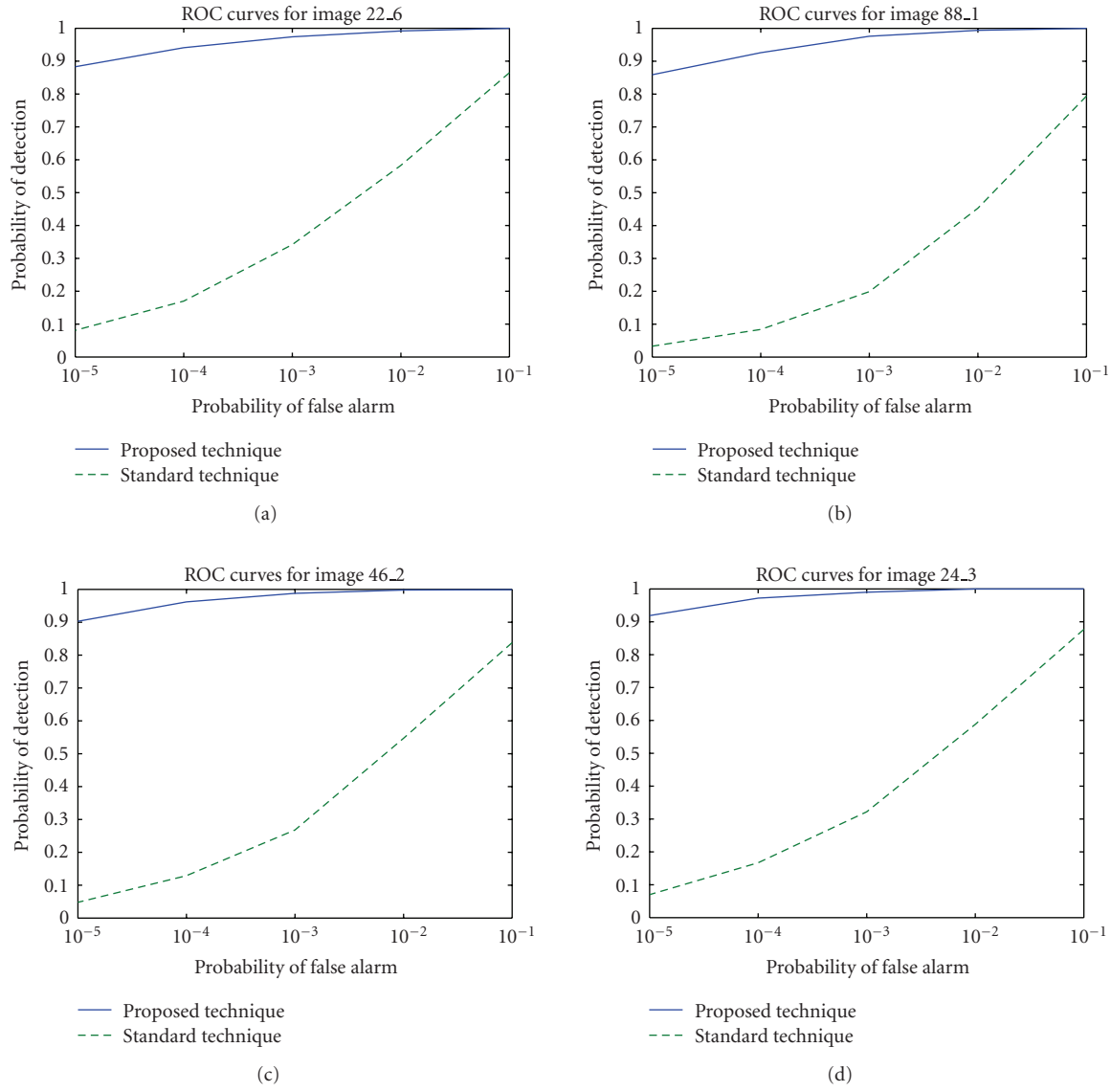


Figure 10: ROC curves of segmented, watermarked images. Watermarking applied in the DFT domain. Strength $\lambda = 0.10$.

segmentation. Comparing Figures 8(a:1) and 8(b:1), the watermark energy in the DWT domain is concentrated into the ridges area (i.e., textured area). However, in the DFT domain, the watermark energy is uniformly spread all over the image. Thus, a severe degradation of the standard detector performance in the DFT domain is expected when applying the segmentation attack, compared to the DWT domain.

After applying the segmentation process on watermarked images, the previous experiment has been carried out and the results obtained are plotted in Figure 9 for the DWT domain and Figure 10 for the DFT domain. For the proposed technique, the ROC curves are exactly the same as for the first experiment, thus, the segmentation process has no influence on the performance of the optimum detector. For the standard technique, the probability of detection decreases significantly and the segmentation process causes a deterioration of detection performance in both DWT and DFT domains. As expected for the DFT domain, the degradation in performance is more significant than that obtained in the DWT domain.

The performance of the proposed technique against common attacks, namely, mean filtering, WSQ compression, and additive white Gaussian noise (AWGN), is also evaluated. Each attack has been applied several times with different strength values. For each attack, the response of the detector to the embedded watermark is plotted along with the threshold. In this way, the influence of each attack strength on the detector response and the corresponding threshold is assessed. The theoretical P_{FA}, which is used to determine the decision threshold, has been fixed at 10^{-7} and the strength λ is set in such a way to obtain a peak signal-to-noise ratio

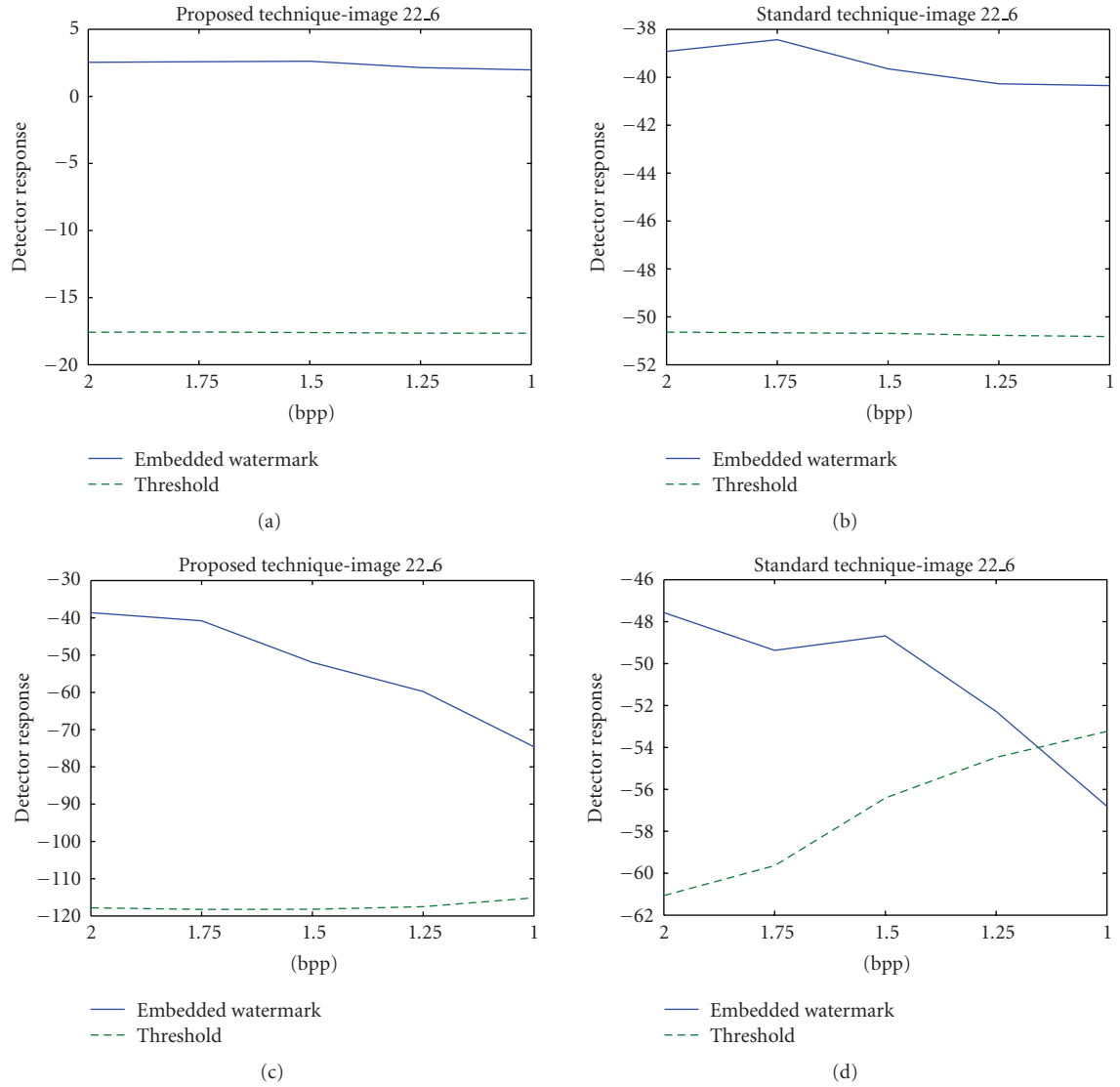


Figure 11: Robustness against WSQ compression. Top: DWT domain. Bottom: DFT domain. Left side graphs: Proposed technique. Right side graphs: Standard technique.

(PSNR) value ≈ 40 for all test images and in both DWT and DFT domains. Only results for one image are plotted since results obtained from other images are very similar.

Robustness against WSQ compression is assessed by iteratively applying the WSQ compression on the watermarked images using the WSQ viewer [23] and varying the bit-rate value measured by bits per pixel (bpp). The results obtained are reported in Figure 11. Obviously, the watermarking in the DWT domain is more robust for both the proposed and the standard techniques since the compression technique is operating in the same domain. On the contrary, the watermarks embedded in the DFT domain do not resist the WSQ compression. Again, the proposed technique outperforms the standard one.

The results of degradations due to AWGN are shown in Figure 12. The watermarked images were corrupted by AWGN with different value of signal-to-noise ratio (SNR). For all images and in both the DWT and the DFT domains, the watermarks are very robust for both the proposed and the standard techniques.

Figure 13 shows the results of watermarked fingerprint images corrupted by mean filtering. The watermarked images were blurred with different filter window size. Although the proposed technique is slightly better than the standard one, the mean filtering affects significantly the detector performance. Note that the detector for the standard technique in the DFT domain is unable to detect the embedded watermarks for all images and all filter window sizes. This is justified by the fact that this type of filtering smooths the image and attenuates the shape of edges and textures.

5. CONCLUSIONS

In this paper, a novel scheme has been proposed to watermark biometric images. This scheme exploits the fact

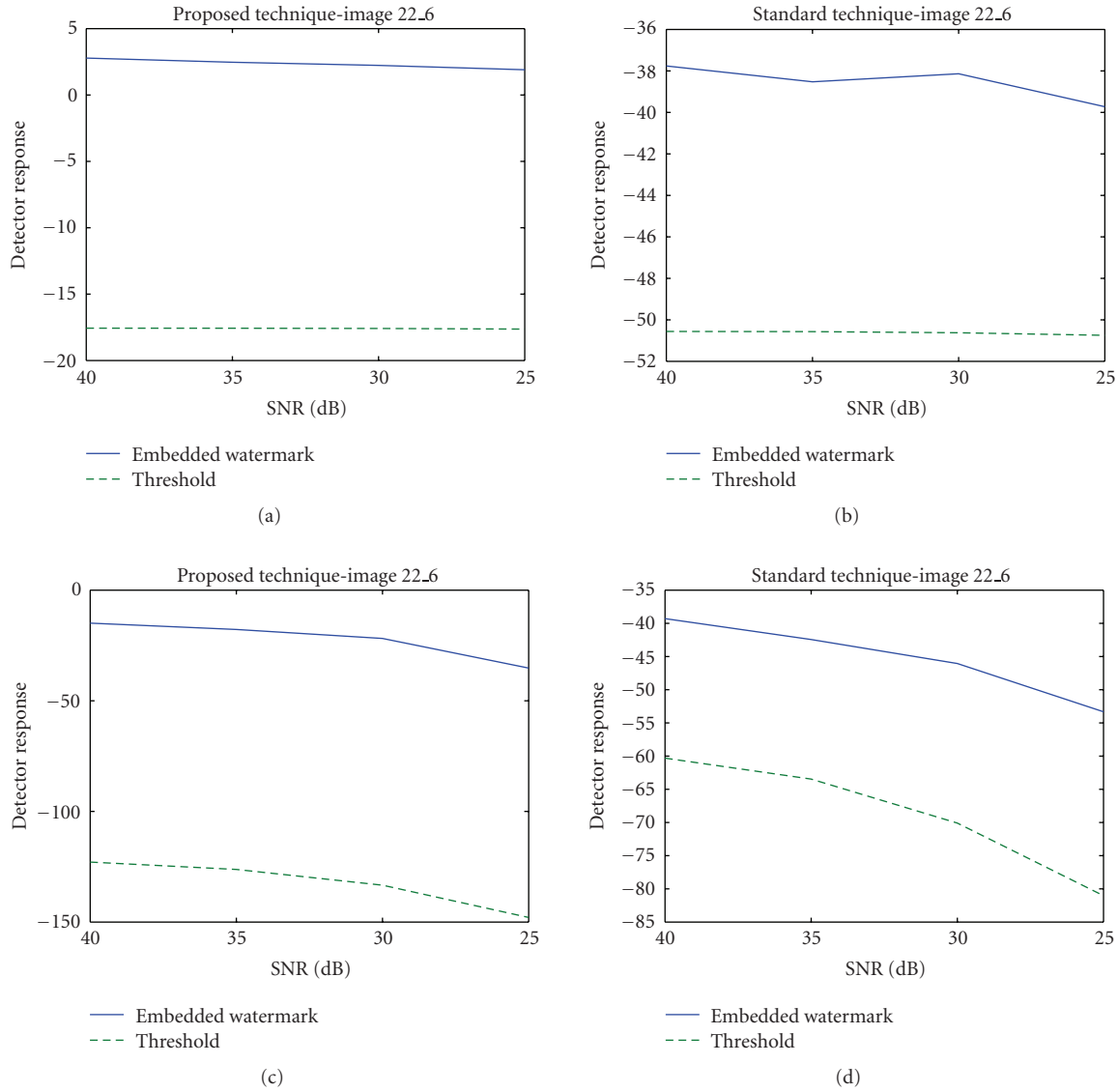


Figure 12: Robustness against additive white Gaussian noise. Top: DWT domain. Bottom: DFT domain. Left side graphs: Proposed technique. Right side graphs: Standard technique.

that biometric images have only one *region of interest*, which constitutes the useful and unique processed region by most of the biometric-based identification/authentication systems. This fact can also be exploited by watermarking techniques where the watermark should be embedded into the region of interest only, instead of spreading it into the whole image. This proposed scheme is motivated by the following: (i) increasing the robustness of the watermark against segmentation and other attacks such as filtering, noise because even the attacker knows that the watermark is embedded in this region, concentrating his attacks on that area degrades significantly its quality, hence, making it useless; (ii) providing more transparency to the embedded watermark since the region of interest is a highly textured area and the human eye is less sensitive to changes in that area. The embedding process for the proposed scheme starts by extracting the region of interest and then embeds the watermark in this area only. This scheme is applied to fingerprint images that are used by one of the most employed and widely deployed biometric systems. To extract the ROI of such images, known as *ridges area*, we modified the segmentation technique proposed by Wu et al. [14].

The proposed scheme is used with the classical optimum, multiplicative watermark detection. For sake of generality, the watermark is applied to the DWT and the DFT domains. The DWT coefficients modeled by the generalized Gaussian distribution, whereas, the DFT coefficients are modeled by the Weibull model. The influence introduced by the proposed scheme on the optimum detectors were assessed through experiments, carried out on real fingerprint images with different characteristics. The results obtained clearly show that the detector performance has been improved compared to the standard technique, which operates on the whole image, and this even in the absence of attacks.

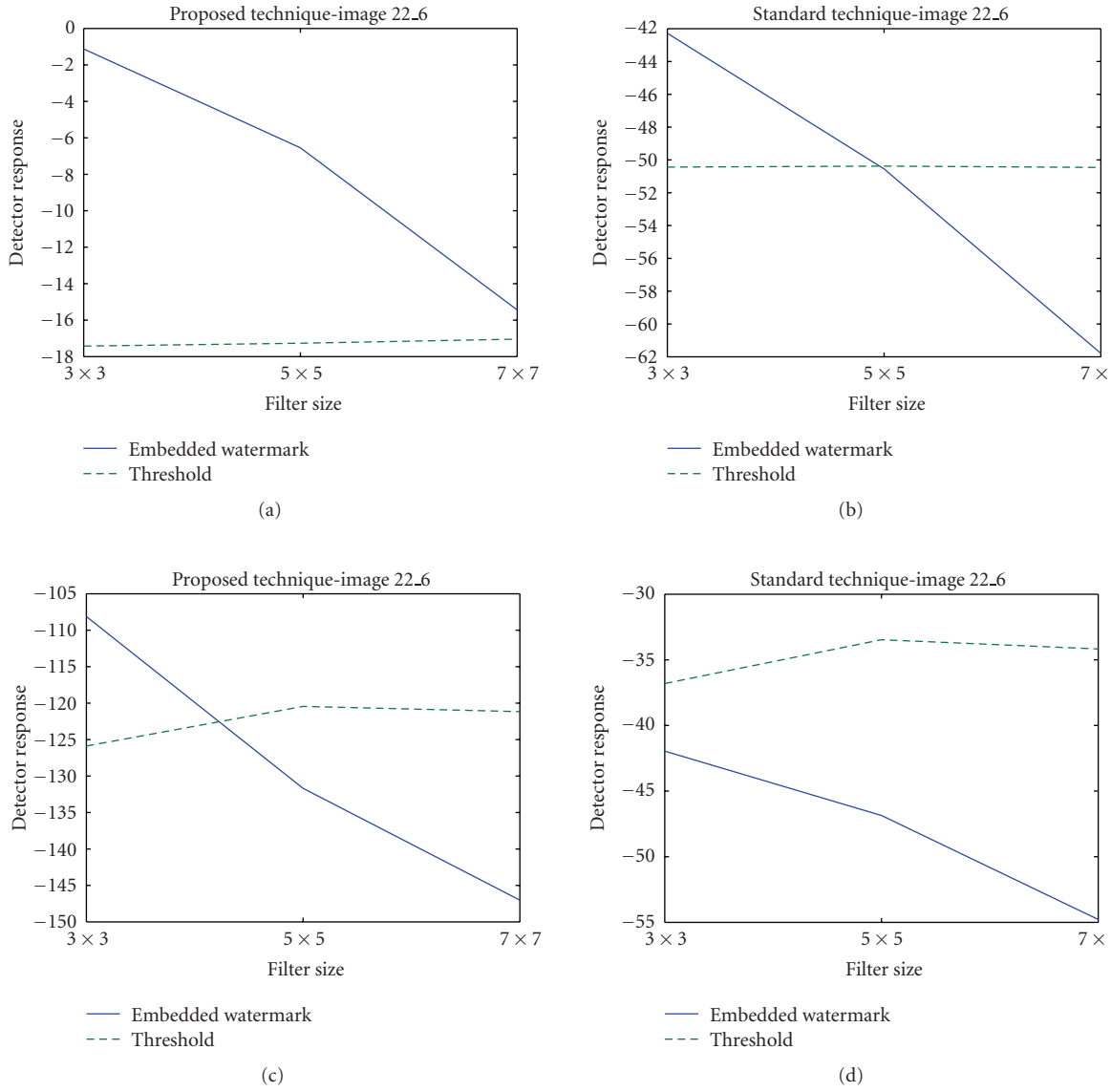


Figure 13: Robustness against mean filtering. Top: DWT domain. Bottom: DFT domain. Left side graphs: Proposed technique. Right side graphs: Standard technique.

In addition, the segmentation technique, which has been applied as a special case of cropping attack, affects the performance of the standard technique since it removes the part of the watermark embedded within the background area. However, this attack has no effect on the proposed technique. Furthermore, the watermarks embedded using the proposed scheme show to be more robust against some other common attacks such as WSQ compression, mean filtering, and white noise addition.

REFERENCES

[1] B. Schneier, "Inside risks: the uses and abuses of biometrics," *Communications of the ACM*, vol. 42, no. 8, pp. 136–139, 1999.

[2] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Proceedings of the 3rd International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA '01)*, vol. 2091 of *Lecture Notes in Computer Science*, pp. 223–228, Halmstad, Sweden, June 2001.

[3] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, New York, NY, USA, 2003.

[4] U. Uludag and A. K. Jain, "Attacks on biometric systems: a case study in fingerprints," in *Security, Steganography, and Watermaking of Multimedia Contents VI*, vol. 5306 of *Proceedings of SPIE*, pp. 622–633, San Jose, Calif, USA, January 2004.

[5] Congress of the United States of America, "Enhanced border security and visa entry reform act of 2002," http://www.unitedstatesvisas.gov/pdfs/Enhanced_Border_SecurityandVisa_Entry.pdf.

[6] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Secure data hiding in wavelet compressed fingerprint images," in *Proceedings of the ACM Multimedia Workshops (MULTIMEDIA '00)*, pp. 127–130, Los Angeles, Calif, USA, October-November 2000.

[7] A. K. Jain and U. Uludag, "Hiding biometric data," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 11, pp. 1494–1498, 2003.

[8] K. Zebbiche, L. Ghouti, F. Khelifi, and A. Bouridane, "Protecting fingerprint data using watermarking," in *Proceedings of the 1st NASA/ESA Conference on Adaptive Hardware and Systems (AHS '06)*, pp. 451–456, Istanbul, Turkey, June 2006.

[9] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data: a state-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 20–46, 2000.

[10] F. Pérez-González, J. R. Hernández, and F. Balado, "Approaching the capacity limit in image watermarking: a perspective on coding techniques for data hiding applications," *Signal Processing*, vol. 81, no. 6, pp. 1215–1238, 2001.

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

[12] M. Barni, F. Bartolini, A. De Rosa, 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, 2001.

[13] Q. Cheng and T. S. Huang, "An additive approach to transform-domain information hiding and optimum detection structure," *IEEE Transactions on Multimedia*, vol. 3, no. 3, pp. 273–284, 2001.

[14] C. Wu, S. Tulyakov, and V. Govindaraju, "Robust point-based feature fingerprint segmentation algorithm," in *Proceedings of the International Conference on Advances in Biometrics (ICB '07)*, vol. 4642, pp. 1095–1103, Seoul, Korea, August 2007.

[15] C. Harris and M. Stephens, "A combined corner and edge detector," in *Proceedings of the 4th Alvey Vision Conference*, vol. 15, pp. 147–151, Manchester, UK, August-September 1988.

[16] N. Otsu, "A threshold selection method from gray-level histograms," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 9, no. 1, pp. 62–66, 1979.

[17] J. V. DiFranco and W. L. Rubin, *Radar Detection*, SciTech Publishing, Raleigh, NC, USA, 2004.

[18] K. Zebbiche, F. Khelifi, and A. Bouridane, "Maximum-likelihood watermarking detection on fingerprint images," in *Proceedings of the ECSIS Symposium on Bio-Inspired, Learning, and Intelligent Systems for Security (BLISS '07)*, vol. 9, pp. 15–18, Edinburgh, UK, August 2007.

[19] T. M. Ng and H. K. Garg, "Wavelet domain watermarking using maximum-likelihood detection," in *Security, Steganography, and Watermaking of Multimedia Contents VI*, vol. 5306 of *Proceedings of SPIE*, pp. 816–826, San Jose, Calif, USA, January 2004.

[20] M. N. Do and M. Vetterli, "Wavelet-based texture retrieval using generalized Gaussian density and Kullback-Leibler distance," *IEEE Transactions on Image Processing*, vol. 11, no. 2, pp. 146–158, 2002.

[21] Q. Cheng and T. S. Huang, "Optimum detection and decoding of multiplicative watermarks in DFT domain," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '02)*, vol. 4, pp. 3477–3480, Orlando, Fla, USA, May 2002.

[22] Fingerprint verification competition, http://biometrics.cse.msu.edu/fvc04db/index.html.

[23] The Wsq viewer (version 2.7), http://www.cognaxon.com/index.php?page=wsqview.