Protecting Fingerprint Data using Watermarking

Khalil Zebbiche, Lahouari Ghouti, Fouad Khelifi and Ahmed Bouridane
School of Electronics, Electrical Engineering and Computer Science
Queen's University Belfast
Belfast,BT7 1NN
Email: {kzebbiche01, L.ghoui, fkhelifi01, A.Bouridane}@qub.ac.uk

Abstract

A motivation for the use of watermarking techniques in biometric systems has been the need to provide increased security to the biometrics data themselves. We introduce an application of wavelet-based watermarking method to hide the fingerprint minutiae data in fingerprint images. The application provides a high security to both hidden data (i.e. fingerprint minutiae) that have to be transmitted and the host image (i.e. fingerprint). The original unmarked fingerprint image is not required to extract the minutiae data. The method is essentially introduced to increase the security of fingerprint minutiae transmission and can also used to protect the original fingerprint image..

1. Introduction

Biometrics is the science of verifying the identity of individual through physiological measurement, e.g., fingerprints, hand geometry, etc. or behavioral traits, e.g., voice and signature. Since biometric identifiers are associated permanently with the user they are more reliable than token based or knowledge based authentication methods such as identification card (can be lost or stolen), password (can be forgotten), etc.

Fingerprints are one of the most mature biometric technologies and are considered legitimate proofs of evidence in courts of law all over the world. Fingerprints are, therefore, used in forensic divisions worldwide for criminal investigations. More recently, an increasing number of civilian and commercial applications are either using or actively considering to use fingerprint-based identification because of a better understanding of fingerprints as well as demonstrated matching performance than any other existing biometric technology [1]. The main stages of a typical fingerprint-based system are: acquisition, representation, feature extraction and matching [2].

Though biometric data provide uniqueness, they do not provide secrecy because biometric data is not replaceable and is not secret. Furthermore, there exist several types of attacks possible in a biometric system. Ratha et al.[3] describe eight basic sources of attack. In addition Schneir[4] identifies many other types of abuses. Watermarking and steganography are possible techniques that can be used to increase the security of the biometric data.

Steganography and watermarking describe methods to embed information transparently into a carrier signal. Staganography is a method that establishes a covered information channel in point-to-point connections, whereas watermarking does not necessarily hide the fact of secret transmission of information from third persons. Besides preservation of the carrier signal quality, watermarking generally has the additional requirement of robustness against manipulations intended to remove the embedded information from the marked carrier object [5].

In this paper, we introduce wavelet-based watermarking method for fingerprint images and this method can be used in steganography-based application to embed minutiae data in fingerprint images. The use of a biometric data (fingerprint image) to hide an other one (fingerprint minutiae) increases the level of security because the unauthorized person who obtains the fingerprint image watermarked is likely to treat the fingerprint image instead the hidden minutiae data.

In the next section, we introduce some image watermarking techniques. Section 3 describes the wavelet-based watermarking method while the experimental results are provided in Section 4. Conclusions and future research are presented in Section 5.

Proceedings of the First NASA/ESA Conference on Adaptive Hardware and Systems (AHS'06)
0-7695-2614-4/06 $20.00 © 2006 IEEE

2. Image watermarking

The basic idea in watermarking is to add a watermark signal to the host data to be watermarked such that the watermark signal is unobtrusive and secure in the signal mixture but can partly or fully be recovered from the signal mixture later on. The image watermarking methods can be classified into two groups according to the domain of application of watermarking: spatial-domain techniques (spatial watermarks) and frequency-domain techniques (spectral watermarks). The spatial-domain techniques directly modify the intensities of image pixels. The simplest spatial-domain image watermarking technique is to embed a watermark in the least significant bits (LSBs) of some randomly selected pixels. The watermark is actually invisible to human eyes. However, the watermark can be easily destroyed if the watermarked image is low-pass filtered or JPEG compressed. To increase the robustness of the watermark, many approaches have been proposed to modify some properties of selected pixels or blocks. The frequency-domain techniques first transform an image into a set of frequency domain coefficients. The transformation may be DCT, Fourier transform, or wavelet transform, etc. The watermark is then embedded in the transformed coefficients of the image such that the watermark is less invisible and more robust to some image processing operations. Finally, the coefficients are inverse-transformed to form the watermarked image.

Watermarking of fingerprint images can be used in applications like: a) Protecting the originality of fingerprint images stored in databases against intentional and unintentional attacks, b) Fraud detection in fingerprint images by means of fragile watermarks (which do not resist to any operations on the data and get lost, thus indicating possible tampering of the data), c) Guaranteeing secure transmission of acquired fingerprint images from intelligence agencies to a central image database, by watermarking data prior to transmission and checking the watermark at the receiver site.

In the literature, there are a few published works for fingerprint image watermarking. A.K.Jain and Uludag.U [6], introduced two applications of an amplitude modulation-based watermarking method in which they hide a user's biometric data in a variety of images. Recently, Ahmed et. al [7] extended the digital watermarking technique Phasemark™ [8] to the important application of fingerprint authentication. The hiding occurs in the Fourier transform frequency domain. Using a signature extracted from the Fourier phase of the original image, they hide an encoded signature back into the original image forming a watermarked image. The detection process computes the Fourier transform of the watermarked images, extracts the embedded signature and then correlates it with a calculated signature. Various correlation metrics determine the identity degree of biometric authentication.

3. Proposed data embedding method

The method used to embed the watermark is an extension of the method proposed by Kundur and Hatzinakos[9] who proposed to embed the watermark in the coefficients of the discrete wavelet transform (DWT) using quantization-based watermarking proposed by Chen and Wornell[10]. We propose to embed the watermark three times in the details coefficients of the highest level discrete wavelet transform of the host image (i.e. fingerprint image). This redundancy of embedding increases the correct extraction rate of the hidden data (i.e. minutiae data). The technique (Figure.4) is comprised of the steps described below:

Step 1: convert the minutiae values (x, y, θ) to be hidden into binary data. Every field of an individual minutia is converted to bit stream data and concatenated to get the watermark W.

Step 2: compute the L^{th}-level discrete wavelet transform of the host image to produce a sequence of $3L$ detail images, corresponding to the horizontal, vertical and diagonal details at each of the L resolution levels, and a gross approximation of the image at the coarsest resolution level. We denote the horizontal, vertical and diagonal detail image component of the highest level resolution by $HD(i,j)$, $VD(i,j)$ and $DD(i,j)$, respectively. The level L is limited by the size of the image and the length of the watermark.

Step 3: select the exact locations of the coefficients to be watermarked. We sort the detail coefficients $HD(i,j)$, $VD(i,j)$ and $DD(i,j)$ in descending order so that,

$$HD_1(i,j) \geq HD_2(i,j) \geq \ldots \geq HD_l(i,j) \quad (1)$$

$$VD_1(i,j) \geq VD_2(i,j) \geq \ldots \geq VD_l(i,j) \quad (2)$$

$$DD_1(i,j) \geq DD_2(i,j) \geq \cdots \geq DD_l(i,j) \quad (3)$$

Where l denotes the length of the watermark W.

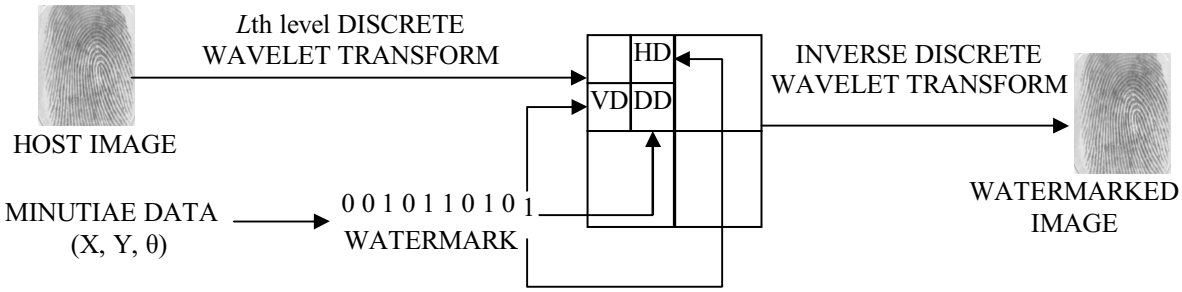


Figure 1. Embedding process to hide the minutiae data.

Step 4: Every watermark bit is embedded in each detail (i.e. horizontal, vertical and diagonal). We embed the watermark by quantizing the coefficients. For this, we divide the range of values between the first and the last coefficient for $HD(i,j)$, $VD(i,j)$ and $DD(i,j)$ into bins of width

$$\Delta_h = \frac{HD_1(i,j) - HD_1(i,j)}{2Q-1} \quad (4)$$

$$\Delta_v = \frac{VD_1(i,j) - VD_1(i,j)}{2Q-1} \quad (5)$$

$$\Delta_d = \frac{DD_1(i,j) - DD_1(i,j)}{2Q-1} \quad (6)$$

Where Δ_h, Δ_v and Δ_d are the width of the bins used for quantizing the coefficients $HD(i,j)$, $VD(i,j)$ and $DD(i,j)$, respectively. Q is defined by the user. The selection of the value of Q involves a trade-off between the robustness and the perceptibility of the watermark. The smaller the value, the more robust to attack the watermark is but the most likely the degradation of the host image will be visible and the watermark will be perceptible. On the other hand, the larger the value of Q, the less likely the watermark will be perceptible; consequently it will make the watermark less resistant to attacks. For example, to embed a watermark of value one to the coefficient $HD_2(i,j)$, this coefficient is quantized to the nearest value shown by circle as shown in Figure 2. Alternatively, to embed a watermark bit of value zero, the coefficient $HD_2(i,j)$ is quantized to the nearest value shown by square.

Step 5: calculate the L^{th} inverse discrete wavelet transform to obtain the watermarked image. We have to ensure the imperceptibility of the watermark.

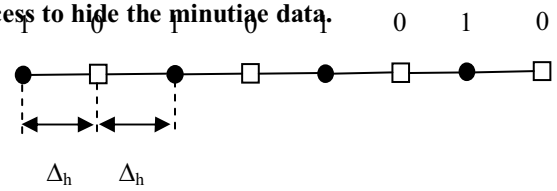


Figure 2. Quantization process to embed the binary watermark.

The watermark extraction aims to reliably estimate the value of the watermark from the host image (i.e. fingerprint image) which possibly has been distorted. The extraction requires the knowledge of the watermark locations, the values of Δ_h, Δ_v and Δ_d, the level of the decomposition to obtain the coefficients. All these requirements make the extraction or the destruction of the watermark more difficult for an attacker. The watermark extraction (Figure3) starts with applying an *L*th level discrete wavelet transform on the watermarked image to obtain the horizontal, vertical and diagonal detail coefficients, denoted $HD_w(i,j)$, $VD_w(i,j)$ and $DD_w(i,j)$, respectively. Because the Watermark W has been embedded three times in the horizontal, vertical and diagonal detail coefficients, we extract W_h, W_v and W_d from $HD_w(i,j)$, $VD_w(i,j)$ and $DD_w(i,j)$, respectively. We then select the coefficients, for $HD_w(i,j)$, $VD_w(i,j)$ and $DD_w(i,j)$, which have been watermarked from the locations using for the embedding. To estimate the value of the watermark bit from a given coefficient, we use the same values Δ_h, Δ_v and Δ_d for embedding to get the closest quantized value to the coefficient and determine if this quantized value was used to embed a bit of value one or zero. The estimated watermark $\tilde{W}$ is obtained by assigning the most common value between W_h, W_v and W_d.

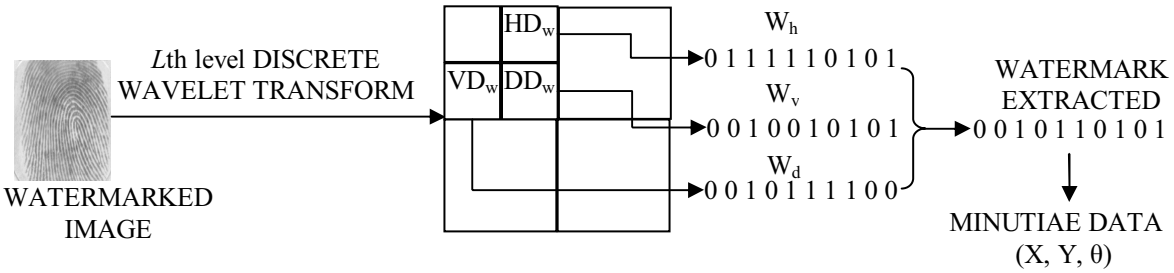


Figure 3. Watermark extraction process.

4. Experimental results

We compared the performance of our method with the method proposed by .K.Jain and Uludag.U [6]. Simulation results were conducted on 10 fingerprint images of size 448×478 arbitrary chosen from 'Fingerprint Verification Competition' (DB_3, FVC2000) database [11]. These images were watermarked with 5 different sets of minutiae data arbitrary chosen. The minutiae data contained three fields per minutiae x-coordinate ([1, 511]), y-coordinate ([1, 511]) and orientation θ ([0, 359]) and every set contained 25 minutiae data. Every field of minutia data converted to 9-bit binary. So every image is watermarked by (25×3×9 = 675 bits). For our method, The images were decomposed using the discrete *Haar* wavelet transform at the 4th level (Figure 4)and the value of $Q = 6$. The watermarking parameters of the method [6] were set to: q = 0.1, A = 100, B = 1000 and every watermark bit was embedded at multiple locations (i.e. 30 locations/bit).

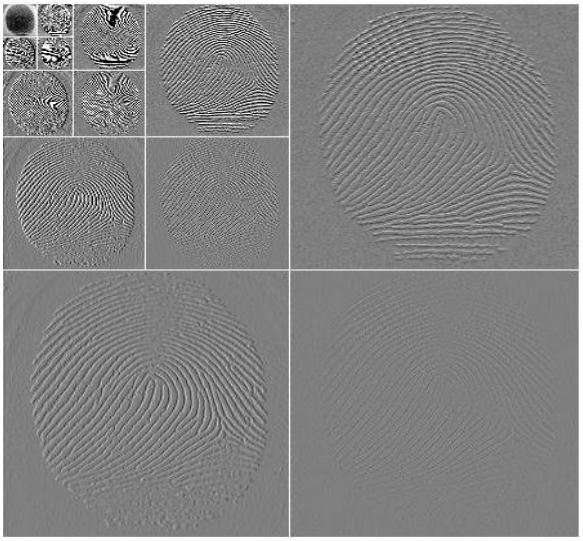
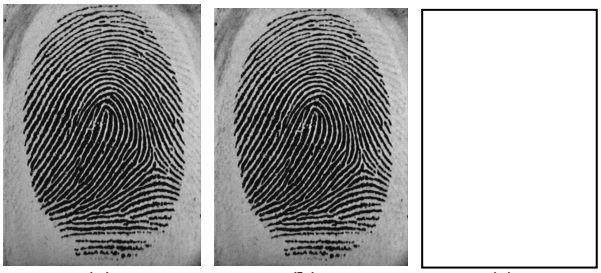


Figure 4. Detail images of the fourth discrete Haar wavelet transform.

Figure 5(c) shows the negative image of the difference between a sample of fingerprint image (Figure 5(a)) and the watermarked one (Figure 5(b)) using the proposed method. For both of the watermarking methods, the watermarked images are visually identical to the original images and the watermark is imperceptible in all images used in the experiments. The extracted minutiae data from all the images is exactly the same as the hidden data.



(a) (b) (c)

Figure 5. Sample fingerprint image: (a) host fingerprint, (b) watermarked fingerprint image, (c) negative image of the difference.

To assess the average magnitude of changes in pixels values, we compute some image characteristics for both methods (Table 1). The first column gives the rate of changed pixels (RCP) between the original and the watermarked image. The second column is the average value for the images pixels (AVP). The third column is the average value for the watermarked pixels (AVWP). The fourth column shows the average change in values of the watermarked pixels (ACVWP). The last column shows the average value of PSNR (peak signal noise ratio) equation (7). It is known that higher the value of PSNR is, less visible is the degradation of the original image due to the watermark.

$$PSNR = 20 \log_{10} \left(\frac{255}{\sqrt{\frac{\sum [f(i,j) - F(i,j)]^2}{NM}}} \right) \quad (7)$$

Where f is the original image, F is the watermarked on and $N \times M$ the size of the image.

Table 1 Host and watermarked images characteristics.

Method	RCP	AVP	AVWP	ACVWP	PSNR
Prop. method	83.02	95.90	95.91	3.31	37.28
Method[6]	9.26	95.90	95.86	13.86	34.75

Simulation results were also conducted to demonstrate the robustness of the proposed technique to JPEG compression, additive noise and two-dimensional linear mean filtering. The robustness of the technique is evaluated by comparing the normalized correlation coefficient of the extracted watermark with the original one. The normalized correlation coefficient is defined as

$$\rho(w,\tilde{w}) = \frac{\sum_{n=1}^{N} w(n)\tilde{w}(n)}{\sqrt{\sum_{n=1}^{N} w^2(n)}\sqrt{\sum_{n=1}^{N} \tilde{w}^2(n)}} \qquad (8)$$

Where w is the original watermark, $\tilde{w}$ is the extracted watermark and N is the length of the watermark. $w(n), \tilde{w}(n) \in \{1,-1\}$ (we replace the watermark bit 0 by -1).

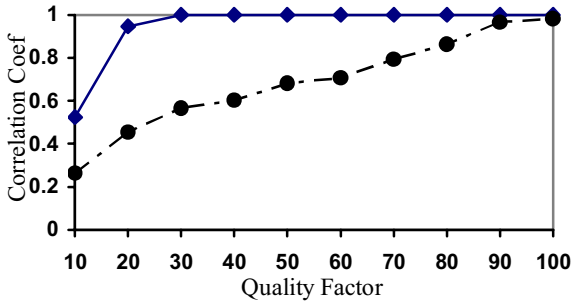
The results of $\rho(w,\tilde{w})$ upon watermark extraction for mean filtering as a function of the filter size K×K, JPEG compression as a function of quality factor and additive noise as a function of signal-to-noise ratio (SNR) are plotted using solid line for the proposed method and dashed lines for the method [6] in Figure 6. We have also calculated the PSNR of the watermarked images after filtering, compression and noise addition to show the degradation of the watermarked images due to these possible attacks.

Figure 6(a) shows the effect of compression on the correlation coefficient. The images were compressed using the MATLB function *imwrite* and varying the quality factor. The correlation coefficients of the proposed method are much higher than that for the method [6]. The extracted watermark is the same as the original one at quality factor of 30 and higher for the proposed method. To show the degradation of the compressed images, we calculate the PSNR for the two methods (see Table 2).

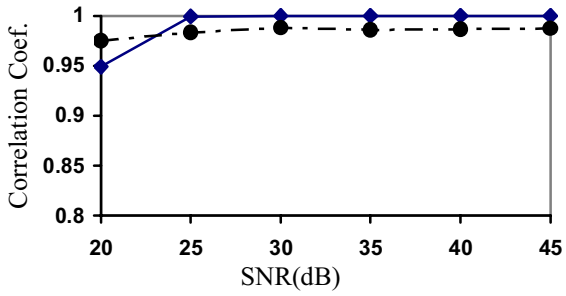
Figure 6(b) provides the results for degradation using additive white Gaussian noise. Both of The methods perform well in the presence of additive noise. Severe visual image degradation occurred at signal-to-noise ratios (SNR) of 20 dB and less. For the proposed method, the correct watermark can be correctly extracted at 25dB and higher. The PSNR of the noised images is given in table 3.

The results for degradations from linear mean filtering are presented in Figure 6(c) and the PSNR of the filtered images is also given in Table 4. When the images are 3×3 mean filtered,beyond which the imperceptibility is affected, the proposed method clearly outperforms the one in [6].

(a) Results for JPEG Compression



(b) Results for Additive Noise



(c) Results for Mean Filtering

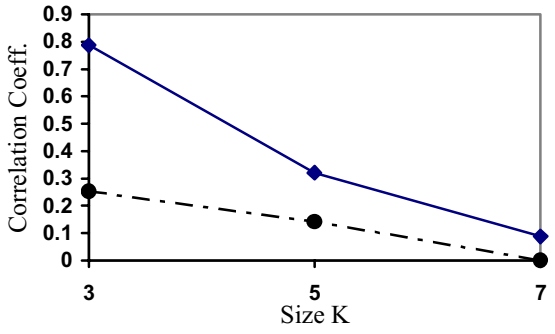


Figure 6. Normalized Correlation Coefficients between the original watermark and the extracted one for varying (a) Compression Ratios, (b) SNRs, (c) Mean linear filtering size. The solid and dashed lines correspond to the proposed method and method [6] respectively.

Table 2. PSNR of the compressed images.

Method \ Qua.Fa	10	20	30	40	50	60	70	80	90	100
Prop. method	26.31	28.06	29.44	30.37	31.12	31.89	32.96	34.60	38.11	58.47
Method[6]	25.27	27.19	28.53	29.44	30.10	30.77	31.72	33.28	37.08	58.45

Table 3. PSNR of the noised images.

Method \ SNR	20	25	30	35	40	45
Prop.method	26.77	31.79	36.77	41.78	46.75	51.78
Method[6]	26.78	31.78	36.78	41.75	46.78	51.78

Table 4. PSNR of the filtered images.

Method \ K	3	5	7
Prop.method	26.15	21.07	18.39
Method[6]	25.67	20.99	18.31

It is worth mentioning that our method is much lower in complexity than the method[6]. The latter processes each pixel in the spatial domain to find the best locations for watermark embedding by computing, for each pixel of interest, standard deviation and gradient magnitude. Table 5 shows the time of embedding/extraction of the watermark for the two methods on Intel processor (2128MHz).

Table 5. The time of embedding/extraction on a 2128 MHz Intel processor.

	Embedding (seconds)	Extraction (seconds)
Proposed method	0.5718	0.1502
Method[6]	73.7924	0.5979

5. Conclusions

In this paper we introduce a multiresolution wavelet-based digital watermarking method to hide biometric data (i.e. fingerprint minutiae data) into fingerprint images. This method doesn't require the original image to extract the embedded minutiae. The experimental results show that the introduced method is highly robust to compression and additive noise and quite resilient to moderate linear mean filtering. Future work will be concentrate on making the method more robust to attacks.

6. References

[1] A.K. Jain and S. Pankanti, "Fingerprint Classification and Matching", *Image and Video Processing Handbook*, A.Bovic, 2000.

[2] A.K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identity authentication system using fingerprints", *Proc. IEEE*, vol. 85, no.9, Sept. 1997, pp. 1356-1388.

[3] N.K. Ratha, J.H. Connell and R.M. Bolle, "An analysis of minutiae matching strength", *Proc. 3rd AVBPA*, Halmstad, Sweden, June 2001, pp.223-228.

[4] B. Schneier, "The Uses and Abuses of Biometrics", *Comm. ACM*, vol. 42, no.8, Aug. 1999, pp. 136.

[5] M. Arnold, M. Schmucker and S.D. Wolthusen, *Techniques and Applications of Digital Watermarking and Content Protection*, Artech House, London,2003.

[6] A.K. Jain and U. Uludag, "Hiding Biometric Data". *Proc. IEEE*, vol. 25, no. 11, Nov. 2004.

[7] F. Ahmed and I.S. Moskovitch, "Composite Signature Based Watermarking for Fingerprint Authentication". *Proc. ACM Multimedia and security Workshop*, NY, Aug. 2005.

[8] F. Ahmed and I.S. Moskovitch, "A Correlation-based Watermarking Method for Image Authentication Application". *Optical Engineering Journal*, Aug. 2004.

[9] D. Kundur and D. Hatzinakos, " Digital Watermarking Using Multiresolution Wavelet Decomposition", *International conference on acoustic Speech and Signal Processing (ICASSP)*, Seattle, May. 1998, pp. 2969-2972.

[10] B. Chen and G.W. Wornell, " Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding", *Proc. IEEE Transactions on Information theory*, vol. 47, No. 4, May. 2001.

[11] Fingerprint Verification Competition http://bias.csr.unibo.it/fvc2002/download.asp FVC Fingerprint database.