14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, September 4-8, 2006, copyright by EURASIP

DATA HIDING IN FINGERPRINT IMAGES

L. Ghouti and A. Bouridane

School of Computer Science, Queen's University of Belfast.
Belfast BT7 1NN, United Kingdom.
Email: {LGhouti01,A.Bouridane}@qub.ac.uk

ABSTRACT

Following the emergence and success of biometric identification systems as a powerful and irrefutable tool for security-aware architectures, it became evident that ensuring the authenticity of the biometric data itself is a challenging research problem. Furthermore, the "*open*" nature of this type of data makes it extremely vulnerable against typical processing attacks present in biometric acquisition hardware and software. In this paper, we propose a robust watermarking system to authenticate the biometric data. To enable the watermark robustness, we embed the watermark payload using the most important features of the biometric images. We propose image edges, determined by the wavelet maxima points, to quantify the robust feature points pertaining to the biometric images. The feature points, wavelet maxima, are modified in a way to ensure watermark imperceptibility while achieving high robustness. Also, geometric-invariance is achieved because the wavelet maxima representations are capable of adjusting the sampling grid when the host images are translated. Finally, performance results are reported to illustrate the robustness of the proposed watermarking system.

1. INTRODUCTION

Security-aware (SA) architectures are becoming increasingly popular to undermine the risks and anticipate the dangers engendered by any terrorist threat. In most available SA systems and frameworks, "*digital biometrics-based*" personal identification techniques, using physiological or behavioral characteristics, are gaining wider acceptance and popularity. Such acceptance and popularity are mainly attributed to the ability of the latter techniques to discriminate between different authorized and impostor individuals. It should be noted that traditional "*token-based*" or "*knowledge-based*" techniques such as identification cards (ID), passwords, etc., have less capabilities than their biometrics-based counterparts. However, the wide-spread acceptance of the biometrics-based technology has given rise to serious concerns about the security and integrity of the biometric data. For instance, unlike the case of credit cards, ID cards, or passwords which can be replaced if stolen, it is not possible to replace a person's biometric data when stolen [1]. In [2], Schneier states that for a biometrics-based verification system to work properly, the verifier system must ensure the legitimate origin of the biometric data at the time of enrollment. Also, due to the "*open*" nature of this type of data, secrecy can not be achieved. In a generic biometric system, eight basic sources of attacks are identified by Ratha et al. [3]. A brief summary of these attacks is outlined in [1]. All of these attacks aim at decreasing the credibility of a biometric system. However, many solutions are possible to counterfeit these attacks. Using such solutions will not only help in harnessing the use of the biometrics-based systems, but in increasing the security of the biometric data itself. Potential candidate solutions are encryption, digital watermarking, and steganography. In this paper, we propose a solution based on digital watermarking to protect the authenticity of fingerprint images. The latter embeds proprietary information, such as owner data and copyright information, in the host content to protect the intellectual property rights of that content [4]. Jain and Uludag [1] propose two applications of an amplitude modulation-based watermarking method to hide a user's biometric data in a variety of host images images. Uludag's method is capable of increasing the security of both the hidden biometric data (e.g., *eigen-face* coefficients) and host fingerprint images. To achieve watermark imperceptibility, image-adaptive weights are used to control the embedding strength. Two spatial domain methods for watermarking fingerprint images are proposed by Gunsel et al. [5]. In the first method, fingerprint features, detected via a gradient orientation analysis, are kept intact and the watermark payload is embedded in the remaining image elements. To avoid affecting the fingerprint classification stage, the second method preserves the singular points in the fingerprint image. A scheme for embedding the watermark payload in the compressed stream of fingerprint images is proposed by Ratha et al. [6]. The embedding operates in the compressed stream generated by the wavelet scalar quantizer (WSQ) standard. The WSQ coefficients are altered in a way to account for possible image degradation. In this paper, we propose a robust watermarking system to authenticate the biometric data. To enable the watermark robustness, we embed the watermark payload using the most important features of the biometric images. The paper organization is as follows. Section

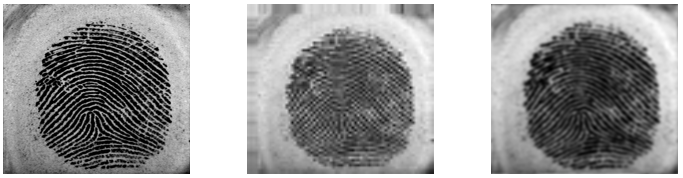

Fig. 1. (a) Fingerprint image. (b) Third-level Approximation subband using orthogonal decomposition. (c) Third-level Approximation subband using nonorthogonal decomposition.

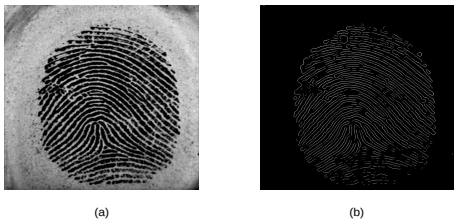

Fig. 2. (a) Fingerprint image. (b) Image edges quantified by wavelet maxima points.

II describes the basic components of the proposed watermarking system. System improvements are detailed in Section III. Then, in Section IV, we present the performance results for fingerprint watermarking in the presence of various accidental and intentional attacks such additive white Gaussian noise (AWGN), Wiener/median filtering, JPEG/JPEG2000 compression. Conclusions and future work directions are drawn in Section V.

2. FINGERPRINT WATERMARKING SYSTEM

A nonorthogonal multiresolution decomposition is used to extract the wavelet maxima [7]. The resulting image decomposition is redundant since the latter decomposition does not involve downsampling after each decomposition stage. The redundant nature of the decomposition represents a major handicap for using such representations in watermarking applications where the payload is embedded by altering the host image coefficients. In this case, the modifications undergone by the host transform are guaranteed to be preserved by the inverse transformation. To alleviate this problem, we adopt, in this paper, a hybrid orthogonal-nonorthogonal image decomposition. Therefore, the resulting decomposition will be smoother than the host image at a coarser scale and robust to compression attacks. In Fig.1, we illustrate the results of three-level orthogonal and nonorthogonal wavelet decompositions on a fingerprint image, respectively. It is clearly illustrated that the approximation subband, based on the latter transform, is smoother than the input image itself unlike the case of the approximation subband resulting from the former transform [7]. Nonorthogonal wavelet transforms are known for their ability to capture the salient signal features (for both 1D and 2D signals) as detailed in [7]. Image edges can be efficiently quantified using such transforms. Fig. 2 shows the fingerprint image and the corresponding thresholded wavelet maxima points.

2.1. Wavelet Maxima Representation

In order to preserve the shift-invariance property, wavelet maxima representations are used for their ability to adapt the sampling scheme by translating the sampling grid when the processed input is translated [7]. Borrowing the underlying principles of Cannys' multiresolution edge detector algorithm, let's define two wavelet functions that are partial derivatives of a two-dimensional smoothing function $\theta(x, y)$ [7]:

$$\psi^1(x,y) = \frac{\partial \theta(x,y)}{\partial x} \quad \text{and} \quad \psi^2(x,y) = \frac{\partial \theta(x,y)}{\partial y} \qquad (1)$$

Then, the wavelet transform of the input image, $I(x, y)$, at a scale $s = 2^j$ has the following two components:

$$W_x^I(s;u,v) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} I(x,y)\psi_s^1(x-u, y-v)\,dxdy \quad (2)$$

$$W_y^I(s;u,v) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} I(x,y)\psi_s^2(x-u, y-v)\,dxdy \quad (3)$$

where $W_x^I(s;u,v)$ and $W_y^I(s;u,v)$ are the wavelet coefficients at location point (u, v) in the x-channel and y-channel components at scale *s*, respectively. Mallat and Zhong [7] show that the two components given in Eqs. 2-3 are proportional to the coordinates of the gradient vector of $I(x, y)$ smoothed by $\theta_s(x, y)$.

2.2. Watermark Embedding Algorithm

As mentioned earlier, we will embed the watermark into the hybrid transform domain obtained after applying two "*orthogonal*" decomposition levels and then one "*nonorthogonal*" decomposition level on the approximation subband of the former block as shown in Fig. 3. First, the host image is decomposed using a two-level orthogonal decomposition followed by one-level nonorthogonal decomposition of the approximation subband. Such hybrid decomposition yields the following subband images: 1) approximation subband image, referred to by $A(u, v)$, 2) horizontal details' subband image, referred to as $W_1(u, v)$ and 3) vertical details' subband image, referred to as $W_2(u, v)$. Then, the subband coefficients of either $W_1(u, v)$ or $W_2(u, v)$ subband that represent the wavelet maxima are selected for watermark embedding using scala QIM quantization [8]. It should be noted that the redundancy of the final image representation represents the main difficulty in the proposed algorithm. In this case, the resulting

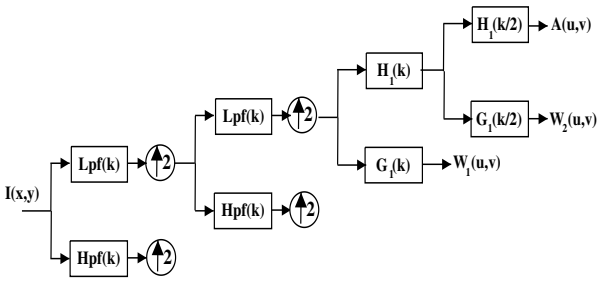

Fig. 3. Watermark embedding block.

Fig. 4. (a) Original fingerprint image. (b) Watermarked image. (c) Difference image.

watermarked subband image may be an *"invalid"* representation and some of the embedded data may be lost after the reconstruction stage. Also, to circumvent the total loss of the embedded data, we use repetition code to increase the probability of data recovery, hence, reducing the probability of false alarms at the decoder stage.

2.3. Watermark Decoding Algorithm

Because the watermark embedding is performed using QIM quantization of wavelet maxima points, the watermark decoding/recovery is quite simple. Similar to the embedding stage, the watermarked image is formed transformed using the same decomposition structure as that shown in Fig. 3. Then, the wavelet maxima points are extracted for re-quantization. Since the watermark data is protected via code repetition, majority rule is applied to decide the decoded bit.

3. ALGORITHM REFINEMENT

Since the proposed watermarking scheme is not expected to operate in friendly environments, further refinements are required in order to enhance its robustness versus hostile attack scenarios. Among the proposed enhancements, the selection of the maxima points should be considered more carefully. The selection procedure should not consider those maxima points that are more likely to be destroyed by moderate or severe image manipulations. The threshold used for the selection of the wavelet maxima points plays a crucial role in the performance of the proposed algorithm. The higher the value of the threshold, the better is the watermark robustness. However, this will put a severe limitation on the number of possible host coefficients and, therefore, the watermark capacity will drop drastically. At the decoder stage, the identification of false wavelet maxima points would lead to an increase in the false alarm probability. A more complex watermark decoder is necessary to combat such limitations.

4. SYSTEM PERFORMANCE

We run experiments to evaluate the performance of the proposed watermarking system using a database of fingerprint images having an identical size of 512×512. However, we report the performance results averaged over all the database images. Furthermore, the watermark payload is embedded using selected wavelet maxima points pertaining to the horizontal details subband only. Fig. 4 shows the watermarking results for a fingerprint image extracted from a standard fingerprint database. Using an image adaptive threshold, the total number of embedded bits is 132 bits and the watermarked image has a PSNR value of 35.63 dB. Furthermore, the watermark payload has been adjusted and embedded in the salient points of the fingerprint image (around edges and sharp details) as evidenced by the difference image shown in Fig. 4-(c). It is quite interesting to note that the procedure for maxima selection has been refined and the total number of retained maxima points has been reduced from 9960 to 1583 points. It should be noted that for the embedded watermark payload, repetition coding has been used to enhance the robustness and reliability of the watermark payload. Throughout the reported results, we will use the bit error rate (BER) as the performance measure to evaluate the proposed algorithm. Fig. 5 shows the system robustness against AWGN attack. Obviously, the proposed scheme exhibits an excellent performance in the presence of AWGN attack. The system performance against Wiener and median filtering is shown in Fig. 6. Various local sizes for the filter window have been tested. We report the performance results for window sizes of 3, 5, 7, and 9, respectively. In Fig. 7, we present results for the performance of the proposed watermarking system in the presence of JPEG 2000 compression. Fig.9 clearly shows that the proposed watermark embedding scheme does not alter the location of the minutiae points which makes the fingerprint matching process unaffected.

5. CONCLUSIONS

In this paper, we have proposed a novel scheme for high-reliability, robust, and high-capacity digital watermarking for fingerprint images. The robustness of the embedded watermark is ensured by the selection of image salient points to carry the watermark payload. Wavelet maxima, better known for edge characterization, are selected as the candidate channel to conceal the embedded watermark. Reported results clearly illustrate the robustness of the proposed scheme against several linear and geometric image manipulations and attacks.

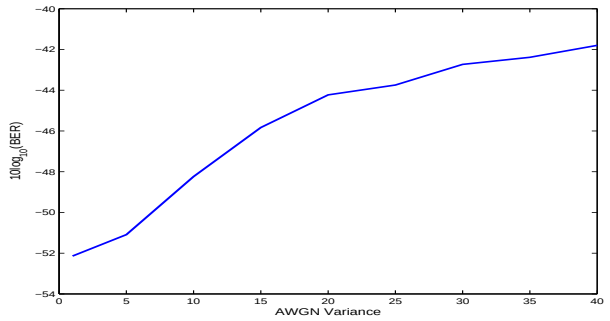

Fig. 5. Mean logarithmic BERs in the presence of AWGN noise.

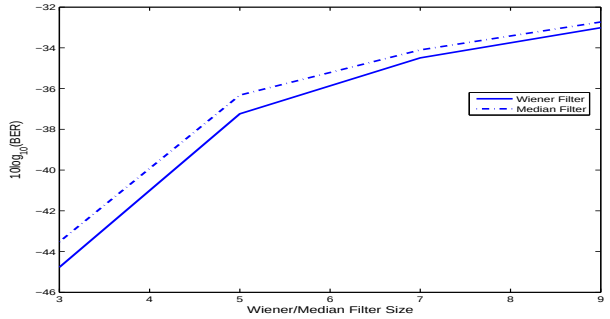

Fig. 6. Mean logarithmic BERs in the presence of Wiener (solid line) and median (dotted line) filtering attack.

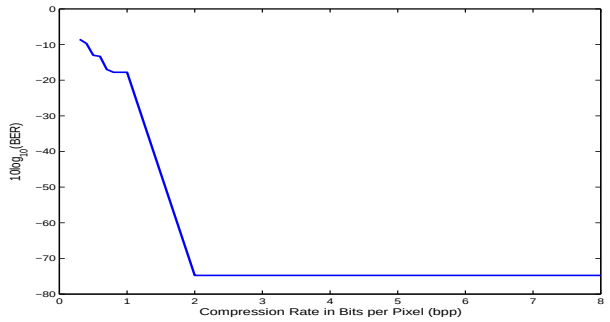

Fig. 7. Mean logarithmic BERs in the presence of JPEG 2000 compression.

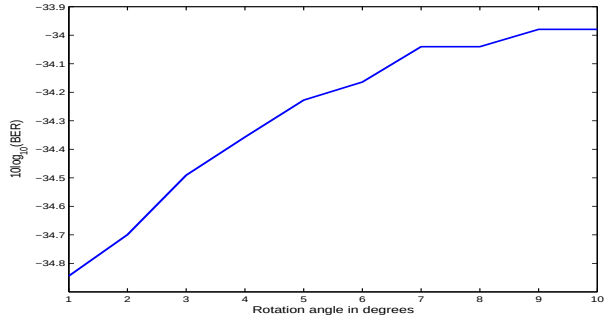

Fig. 8. Mean logarithmic BERs in the presence of rotation attack.

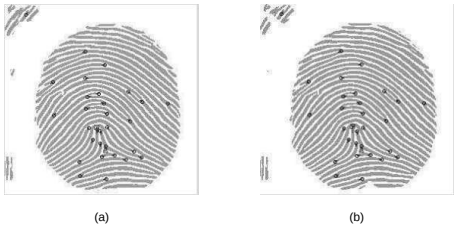

Fig. 9. (a) Original fingerprint image with overlaid minutiae. (b) Watermarked fingerprint image with overlaid minutiae.

Furthermore, the outlined algorithm enjoys high imperceptibility as evidenced by the PSNR values of the watermarked images and the main fingerprint features, used in the classification and matching block, are not affected by the embedding algorithm. Finally, as a possible future extension of the present work, a robust perceptual image hashing scheme may be developed using wavelet maxima as feature points for the construction of perceptually robust hash strings.

6. REFERENCES

[1] A. K. Jain and U. Uludag, "Hiding biometric data," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 25, no. 11, pp. 1494–1498, Nov. 2003.

[2] B. Schneier, "The uses and abuses of biometrics," *Comm. ACM*, vol. 42, no. 8, p. 136, Aug. 1999.

[3] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An Analysis of minutiae matching strength," in *Proc. Third Intl. Conf. Audio- and Video-Based Biometric Person Authentication*, pp. 223–228, Jun. 2001.

[4] L. Ghouti, A. Bouridane, M. K. Ibrahim, and S. Boussakta, "Digital image watermarking using balanced multiwavelets," *IEEE Trans. on Signal Processing*, vol. 54, no. 3, pp. XXX–XXX, Mar. 2006.

[5] B. Gunsel, U. Uludag, and A. M. Tekalp, "Robust watermarking of fingerprint images," *Pattern Recognition*, vol. 35, no. 12, pp. 2739–2747, Dec. 2002.

[6] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Secure data hiding in wavelet compressed fingerprint images," in *Proc. ACM Multimedia*, pp. 127–130, Oct. 2000.

[7] S. Mallat, *A Wavelet Tour of Signal Processing*. Academic Press, Second Edition, 1999.

[8] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Trans. Inform. Theory*, vol. 47, no. 5, pp. 1423–1443, May 2001.