Hiding a Face in a Fingerprint Image

Anil K. Jain, Umut Uludag and Rein-Lien Hsu
Computer Science and Engineering Department, Michigan State University
3115 Engineering Building, East Lansing, MI, 48824, USA
{jain, uludagum, hsureinl}@cse.msu.edu

Abstract

With the wide spread utilization of biometric identification systems, establishing the authenticity of biometric data itself has emerged as an important research issue. We present a fingerprint image watermarking method that can embed facial information into host fingerprint images. This scheme has the advantage that in addition to fingerprint matching, the recovered face during the decoding can be used to establish the authenticity of the fingerprint and the user. By computing the ROC curves on a fingerprint database of 160 individuals, we show the advantages of the proposed watermarking scheme. Further, our scheme does not introduce any significant degradation in the fingerprint matching performance.

1. Introduction

Traditional token-based or knowledge-based personal identification techniques are unable to differentiate between an authorized person and an impostor who fraudulently acquires the access privilege of an authorized person. Biometrics technology is based on using physiological or behavioural characteristics in personal identification, and can easily differentiate between an authorized person and a fraudulent impostor [4]. While the biometrics techniques offer a reliable method for personal identification, the problem of security and integrity of the biometrics data poses new issues. For example, if a person's biometric data (e.g., his/her fingerprint image or fingerprint features) is stolen, it is not possible to replace it as compared to replacing a stolen credit card, ID or password. Schneier [9] points out that, a biometrics-based verification system works properly only if the verifier system can guarantee that the biometric data came from the legitimate person at the time of enrollment.

In order to promote the wide spread utilization of biometric techniques, an increased level of security of biometric data is necessary [7]. Encryption and watermarking are among the possible techniques to achieve this. Encryption does not provide security once the data is decrypted. On the other hand, watermarking involves embedding information into the host data itself, so it can provide security even after decryption. Furthermore, encryption can be applied to the watermarked data. However, embedding watermark may change the inherent characteristics of the host image (e.g., locations of minutia points in fingerprints). Therefore, the verification performance based on (decoded) watermarked images should not be inferior compared to performance based on non-watermarked images. We present a watermarking method that embeds facial information of a user in his/her fingerprint images. In this way, the authenticity of the fingerprint can be established.

2. Fingerprint Watermarking Techniques

There have been only a few published papers on fingerprint image watermarking. Ratha *et al*. [8] proposed a data hiding method, which is applicable to fingerprint images compressed with WSQ wavelet-based scheme. Pankanti and Yeung [6] proposed a fragile watermarking method for fingerprint image verification. A watermark image is embedded in the fingerprint image, by utilizing a verification key. Their method can localize any region of the image that has been tampered. To increase the security of the watermark data, the original watermark image is first transformed into another mixed image, and this mixed image is used as a new watermark image. The mixed image does not have a meaningful appearance, contrary to original watermark image which can contain specific logo or text. Pankanti and Yeung show that their watermarking technique does not lead to a significant performance loss in fingerprint verification. A semi-unique key based on local block averages is used by Jain [2] to detect tampering of host images, including fingerprints and faces. Uludag *et al.*'s [11] watermarking methods preserve the quantized gradient orientations at and around watermark embedding locations (so all of the fingerprint features extracted using gradient information are preserved) and singular points in the fingerprint image.

3. Facial Information as Watermark

Embedding facial information into a fingerprint image can enhance the security of a fingerprint-based personal authentication system. In a typical application scenario, the fingerprint image of a person will be stored in a smart card that he/she carries. At an access control site, the fingerprint of the user will be sensed and it will be compared to the fingerprint stored on his/her smart card. Along with this fingerprint matching, our proposed scheme will extract the face information hidden in the fingerprint image. The recovered face will be used as a second source of authenticity either automatically or by a human in a supervised biometric application. The block diagram of the proposed system is given in Figure 1.

The amplitude modulation based watermarking method described here is an extension of the blue channel watermarking method of Kutter *et al.* [5]. Our method includes image adaptivity, fingerprint feature analysis (e.g., minutiae and ridges) and watermark strength controller along with the basic method in [5]. First, the watermark data is converted to a bit stream. For facial information, this bit stream is obtained from the eigen-face coefficients [10]. The fingerprint pixel values are changed according to the following equation.

$$P_{WM}(i,j) = P(i,j) + (2s-1)P(i,j)q\left(1+\frac{SD(i,j)}{A}\right)* \left(1+\frac{GM(i,j)}{B}\right)\beta(i,j), \quad (1)$$

where $P_{WM}(i,j)$ and $P(i,j)$ are (i,j) th pixel values in the watermarked and original images, respectively. The value of watermark bit is denoted as s and watermark embedding strength is denoted as q, $s \in [0,1]$, $q > 0$. $SD(i,j)$ denotes the standard deviation of pixel values in the neighborhood of pixel (i,j), and $GM(i,j)$ denotes the gradient magnitude at (i,j). A and B are weights for the standard deviation and gradient magnitude, respectively. The $\beta(i,j)$ term guarantees that image pixels, called marked pixels, whose alteration may affect fingerprint verification performance are unchanged; $\beta(i,j)$ takes the value 0 if the pixel (i,j) is a marked pixel and has the value 1, otherwise. The marked pixels are defined by either minutiae analysis or ridge analysis of the fingerprint image.

Every watermark bit with value s is embedded at multiple locations in the input fingerprint image. A random number generator initialized with the secret key generates locations of the pixels to be watermarked. In addition to the watermark data, two reference bits, 0 and 1, are also embedded into the image. These reference bits help in calculating an adaptive threshold in determining the watermark bit values during decoding.

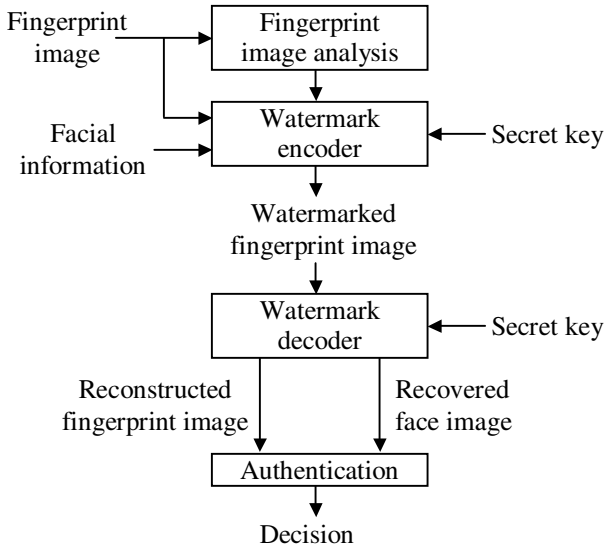

Figure 1. Hiding a face in a fingerprint.

Decoding starts with finding the embedding locations in the watermarked image, via the secret key used during the encoding stage. For every embedding location (i,j), its value is estimated as the linear combination of pixel values in a cross-shaped neighborhood of the watermarked pixels as

$$\hat{P}(i,j) = \frac{1}{4c}\left(\sum_{k=-c}^{c} P_{WM}(i+k,j) + \sum_{k=-c}^{c} P_{WM}(i,j+k) - 2P_{WM}(i,j)\right), \quad (2)$$

where c determines the size of this neighborhood; $c = 2$ in our experiments. The difference between the estimated and watermarked pixel values is calculated as

$$\delta = P_{WM}(i,j) - \hat{P}(i,j). \quad (3)$$

These differences are averaged over all the embedding locations associated with the same bit, to yield $\bar{\delta}$. For finding an adaptive threshold, these averages are calculated separately for the reference bits, 0 and 1, as $\bar{\delta}_{R0}$ and $\bar{\delta}_{R1}$, respectively. Finally, the watermark bit value $\hat{s}$ is estimated as

$$\hat{s} = \begin{cases} 1 & \text{if } \bar{\delta} > \dfrac{\bar{\delta}_{R0} + \bar{\delta}_{R1}}{2} \\ 0 & \text{otherwise.} \end{cases} \quad (4)$$

In Eq. (1), the value of $SD(i,j)$ is computed as the standard deviation of the pixel values in a cross-shaped (5x5) neighborhood of the embedding location (i,j). The

gradient magnitude $GM(i,j)$ term is computed via the 3x3 Sobel operator. These terms adjust the strength of watermarking by utilizing local image information.

The watermark decoding process can produce erroneous bits since decoding is based on an estimation procedure. In order to increase the decoding accuracy, the encoder uses a controller block which adjusts the strength of watermarking, q, on a pixel-by-pixel basis. From the decoded watermark bits, the face image hidden in the fingerprint is reconstructed by using decoded eigen-face coefficients and the eigen-faces stored at the watermark decoding site. In addition, an estimate of the original fingerprint image is found via replacing the watermarked pixel values with the $\hat{P}(i,j)$ estimate. The reconstructed fingerprint image and decoded face image are used in authentication modules; the face image can also be examined by an operator in a supervised (attended) biometric application.

4. Experimental Results

Figure 2 shows various stages of watermark encoding and decoding for the host fingerprint image (300x300) shown in Figure 2(a). Input face image (150x130) is shown in Figure 2(b). The watermark information occupies 56 bytes, corresponding to the 14 eigen-face coefficients (4 bytes per coefficient). These 14 eigen-face coefficients generate the 150x130 watermark face image of Figure 2(c) [1]. Note that 14 eigen-face coefficients are sufficient for a high fidelity reconstruction of input face (compare Figures 2(b) and 2(c)). The eigen-face coefficient vector which is embedded in Figure 2(a) is [-39.06 -29.71 17.44 -49.33 -12.07 19.66 -0.42 -2.10 4.07 -6.49 4.44 2.31 -13.24 2.74]. A small face database, which consists of 40 images, with four images each of 10 subjects, was used to generate the eigen-faces and coefficients.

Figures 2 (d)-(f) correspond to minutiae-based data hiding. The input image in Figure 2(a) is watermarked without changing the pixels that fall in black squares (16% of all image pixels) in Figure 2(d). The image of Figure 2(d), which represents $\beta(i,j)$ term in Eq. (1), is obtained by drawing 23x23 square blocks around every minutiae of input fingerprint image. Figure 2(e) is the watermarked image and Figure 2(f) shows the image reconstructed during watermark decoding. Nearly 15% of fingerprint pixels are modified during watermark encoding. Figures 2 (g)-(i) correspond to ridge-based data hiding: The input image in Figure 2(a) is watermarked without changing the pixels which fall in black lines (31% of all image pixels) in Figure 2(g). The image of Figure 2(g) is obtained from the thinned ridge image of the input fingerprint via dilation with a 3x3 structuring element. Figure 2(h) is the watermarked image and Figure 2(i) shows the image reconstructed during watermark decoding. Nearly 15% of fingerprint pixels are modified during watermark encoding.

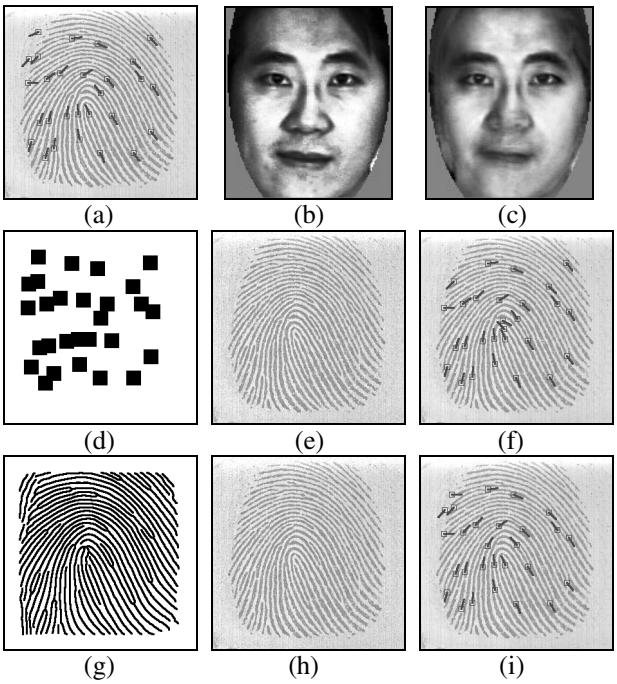

Figure 2. Facial information embedding and decoding: (a) input fingerprint image with overlaid minutiae, (b) input face image, (c) watermark face image, (d) feature image based on minutiae, (e) image in (a) watermarked using (d), (f) reconstructed fingerprint with overlaid minutiae, (g) feature image based on ridges, (h) image in (a) watermarked using (g), (i) reconstructed fingerprint with overlaid minutiae.

The key used in generating the locations of the pixels to be watermarked is selected as the integer 1,000. However, the exact value of the key does not affect the performance of the method. Other watermarking parameters are set to: $q = 0.1$, $A = 100$, $B = 1000$. The watermark data is decoded correctly in the decoding phase in both cases; the recovered faces are exactly the same as the watermark face image in Figure 2(c).

In order to assess the effect of watermarking on fingerprint verification accuracy, the reconstructed fingerprint images shown in Figures 2(f) and 2(i) and the original image shown in Figure 2(a) are compared using the fingerprint matcher described in [3]. The matcher gives a score of 81 and 72, respectively, out of a maximum possible value of 100. ROC curves for original images and images that are recovered after watermark decoding are also computed. A total of 640 fingerprint images are used in our experiments. These images come

from 160 users, with 4 impressions each of the right index finger captured using a Veridicom sensor. Three ROC curves given in Figure 3 correspond to fingerprint verification (i) without watermarking, (ii) with minutiae-based watermarking and (iii) with ridge-based watermarking. The similarity of the ROC curves in Figure 3 indicates that both of the watermarking methods do not introduce any significant degradation in fingerprint verification accuracy. Furthermore, the embedded information (i.e., 14 eigen-face coefficients) was decoded with 100% accuracy in all the 640 watermarked images.

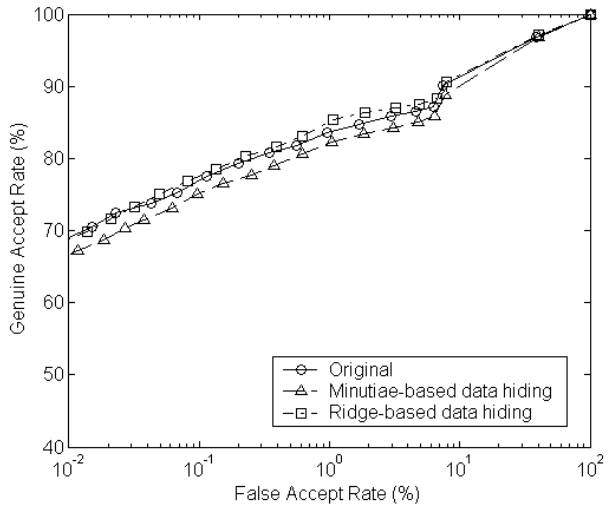

Figure 3. ROC curves.

Table 1 shows the averages of image pixel value, changed pixel value, absolute pixel change, changed pixel ratio and feature pixel ratio, calculated for the 640 host fingerprint images.

Table 1. Host image and watermark statistics

Averages	Image pixel value	Changed pixel value	Absolute pixel change	Changed pixel ratio	Feature pixel ratio
Case (ii)	203.9	205.2	23.9	16%	13%
Case (iii)	203.9	200.2	23.3	16%	26%

The number of eigen-face coefficients (i.e., 14) was selected by considering watermark robustness vs. face image quality trade-off. A higher number of coefficients will lead to more precise reconstruction of face images, but due to the increase in watermark data size, the robustness of the watermarking scheme will decrease. The proposed watermarking method is robust (not fragile), which means that it can tolerate certain types of attacks, namely image cropping and JPEG compression. For example, even if the watermarked image is significantly cropped, the embedded face can be recovered. However, the minutiae-based matching using the cropped image will lead to a very low matching score. This means that, the ownership of the fingerprint can always be verified by comparing facial image of the user and the recovered face. Our experiments indicate that the embedded face image can be recovered without any loss from 40% cropped watermarked fingerprint images and JPEG compressed (quality factor 80) watermarked fingerprint images.

5. Conclusions

A novel watermarking method for fingerprint images, in which we embed facial information into fingerprints, is described. The watermark data, which consists of the eigen-face coefficients of a user's face, can be used in authenticating the host fingerprint image. The data is hidden in such a way that the fingerprint features that are used in matching are not significantly changed during encoding/decoding. As a consequence, the verification accuracy based on decoded watermarked fingerprint images is very similar to that with original fingerprint images. The robustness of the method against several possible attacks on watermarked images helps in authentication of attacked images.

References

[1] Evaluation of face recognition algorithms. [Online]. www.cs.colostate.edu/evalfacerec/index.html.

[2] S. Jain, "Digital watermarking techniques: a case study in fingerprints & faces", *Proc. ICVGIP 2000*, Bangalore, India, Dec. 2000, pp. 139-144.

[3] 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. 1365-1388.

[4] A.K. Jain, S. Pankanti, and R. Bolle (eds.), *BIOMETRICS: Personal Identification in Networked Society*, Kluwer, 1999.

[5] M. Kutter, F. Jordan, and F. Bossen, "Digital signature of color images using amplitude modulation", *Proc. SPIE EI 1997*, San Jose, CA, Feb. 1997, vol. 3022, pp. 518-526.

[6] S. Pankanti and M.M. Yeung, "Verification watermarks on fingerprint recognition and retrieval", *Proc. SPIE EI 1999*, San Jose, CA, Jan. 1999, vol. 3657, pp. 66-78.

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

[8] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Secure data hiding in wavelet compressed fingerprint images", *Proc. ACM Multimedia 2000 Workshops*, Los Angeles, CA, 2000, pp. 127-130.

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

[10] M. Turk and A. Pentland, "Eigenfaces for recognition", *J. Cognitive Neuroscience*, vol. 3, no. 1, Mar. 1991, pp. 71-86.

[11] U. Uludag, B. Gunsel, and M. Ballan, "A spatial method for watermarking of fingerprint images", *Proc. First Intl. Workshop on Pattern Recognition in Information Systems*, Setúbal, Portugal, July 2001, pp. 26-33.