Parallel-Bit Stream for Securing Iris Recognition

PROF. Dr. Elsayed Mostafa[1], Dr. Maher Mansour[2] and Eng. Heba Saad[3]

[1]Faculty of engineering in Helwan, Helwan university
Cairo, Egypt

[2]Faculty of engineering in Helwan, Helwan university
Cairo, Egypt

[3]Shorouk academy
Cairo, Egypt

Abstract

Biometrics-based authentication schemes have usability advantages over traditional password-based authentication schemes. However, biometrics raises several privacy concerns, it has disadvantages comparing to traditional password in which it is not secured and non revocable. In this paper, we propose a fast method for securing revocable iris template using parallel-bit stream watermarking to overcome these problems. Experimental results prove that the proposed method has low computation time and is available to protect iris template and enhance the security of the iris recognition system.

Keywords: *Biometrics, Watermarking, Revocable Iris Template, Bit Stream.*

1. Introduction

Securing information and ensuring the privacy of personal identities is a growing concern in recognition systems. Traditional authentication schemes primarily based on some secret knowledge possessed by the user for verifying his identity. While these techniques are very popular, they have several limitations. These knowledge-based approaches can not differentiate between an authorized user and a person having access to the passwords. Biometrics-based authentication schemes using fingerprint, iris, face recognition, etc., overcome these limitations while offering usability advantages and are therefore rapidly extending traditional authentication schemes. However, despite its obvious advantages, the use of biometrics raises several security and privacy concerns as outlined below:

1. Biometrics is authentic but not secret: Unlike passwords that are known only to the user where face, voice, and iris biometrics can be captured without the user's explicit knowledge and artificial fingerprints can be used.
2. Biometrics cannot be revoked or canceled: Since they are unique and cannot be reissued, updated, or destroyed if compromised rather than the passwords.
3. If a biometric is lost once, it is compromised forever: Since If a biometric is compromised in one application; essentially all applications where the particular biometric is used are also compromised, while with traditional authentication schemes, the user can maintain different passwords to prevent this.

In order to increase the security of the biometric data, encryption and data hiding technologies are possible to achieve it. Encryption focuses on methods to make encrypted information meaningless to unauthorized parties [1], and data hiding is different in its goal hiding critical information in unsuspected carrier data. Namely, data hiding is based on concealing the information itself. Data hiding techniques reduce the chance of biometric data intercepted by attackers, hence reducing the chance of illegal uses.

Evolving from encryption and data hiding techniques, digital watermarking techniques can be used to embed proprietary information in host data to protect the intellectual property rights of the data.

In [2], the authors compared four watermarking techniques (Least Significant Bit (LSB) substitution, Modified Correlation based algorithm (MCBA), Modified 2D Discrete Cosine Transform (M2DCT), and Discrete Wavelet Transform (DWT)) used to embed an iris template into a face cover. The results show that the DWT based watermarking technique performs best on most of the attacks followed by M2DCT and then MCBA. LSB substitution is relatively easy in embedding the iris template but is extremely sensitive to frequency attacks.

In [3], an iris template is hidden in a face image by FFT (Fast Fourier Transform) based watermarking technique

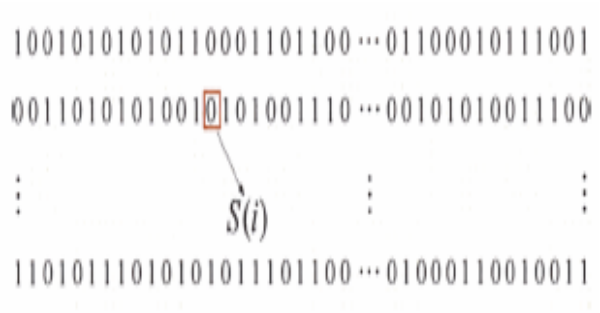
where the frequency amplitudes of iris features is added to those of face image.
In [4], the authors combine the DWT and LSB substitution to achieve robustness against both geometric and frequency watermarking attacks.

Cancelable biometrics [5] refers to the scheme storing a transformed biometric template instead of the actual one. These transformations depend on parameters that can be changed if the database is compromised and a new set of templates need to be issued.
Different ways to provide revocability was suggested in [6, 7, 8]. In [6], an iris template shuffling algorithm is proposed, in which a shuffling key is generated using a password. Iris template is divided into blocks where number of blocks is equal to number of bits in the shuffling key. Then if a bit in the shuffling key is 1, corresponding iris template block is moved to the beginning, and otherwise it is moved to the end.
In [7], two different methods are proposed on both the unwrapped (normalized) iris image and the iris template. The first method uses only the information from the iris itself, while the second method uses external random information for transformation. In the first method, rows in unwrapped iris image are shifted circularly in the horizontal direction using random offsets (first part of the transform key), and then two randomly selected rows (second part of the key) are combined together using an operator like addition or multiplication. For the iris template, the row shifting is similar as unwrapped iris image, but the combination operation is changed to XOR or XNOR. In the second method, the unwrapped iris image or the iris template is mixed by an artificial (key) pattern. The artificial pattern can be pure random noise, a random pattern with iris-like texture, or a synthetic iris pattern. For unwrapped iris image, the two images (unwrapped iris image and artificial pattern) are combined pixel-wise using addition or multiplication. For the iris template, the combination with the key pattern is similar but by using XOR.
In [8], a user specific key is used to determine a reference bit in the iris template. All rows in the template are then connected end to end to form a roll.

2. Bit Stream-Based Iris Template Hiding

In [8] authors proposed a new data hiding method based on bit stream to embed an iris template into a face image. The details of this method are as follows:
As in "Fig. 1", an iris template *I (k, l)* is a binary matrix where an element of the matrix means a bit. For revocability any bit is discretionally chosen as the reference bit (for example, the bit blocked a small rectangle in "Fig. 1") and its value is denoted as *S(i)* where *S(i)* $\in\{0,1\}$ and *i* denotes the bit's location in the matrix that recorded in the secret key. Then the bits in all rows are connected end to end to form a roll.

Fig. 1 An iris feature template.



A face gray image *F(m, n)* (which is the intersection of gray levels from 0 to 255) is a matrix comprising M rows and N columns as the host image, in which every pixel in the host image is represented by 8-bit called byte element. As in "Fig. 2", the pixel blocked a white rectangle is discretionally chosen as the original (reference) byte and its value is denoted as *P(j),* and *j* denotes the pixel's location in the image is recorded in the secret key. The value of *P(j)* is represented by a byte as the rectangle frame pointed by the arrow in the right part of the "Fig. 2". In the rectangle frame, all 8 bits of a byte are shown from the low bit to the high bit ranking from the number 0 to 7 under the rectangle, respectively. The pixels are connected end to end, too.

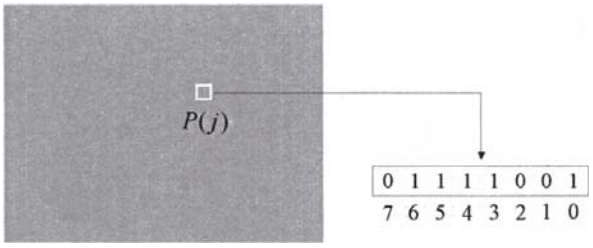


Fig. 2 The host image.

In the encoding stage, beginning from the original bit and original byte, each bit of the iris template data (embedded data or watermark data) is serially embedded in a pixel of the face image (host image) until all bits are embedded into the host image clockwise (or anticlockwise). The encoding process is as Eq. (1).

$$P_{WM}^{(0)}(j) = \begin{cases} 0, & if \quad S(i) = P^{(1)}(j) \\ 1, & if \quad S(i) \neq P^{(1)}(j) \end{cases} \quad (1)$$

Where the superscript in the bracket in $P^{(0)}(j)$ and $P^{(1)}(j)$ means the location in the byte, and the subscript WM means watermarked.
According to Eq. (1), when $S(i)$ is embedded into $P(j)$, the value of $P^{(0)}(j)$ is replaced by $P_{WM}^{(0)}(j)$ and all other bits in $P(j)$ and $P_{WM}(j)$ are the same.

The decoding stage (extracting the iris template data from the face image) starts with finding the beginning location (j) of the data hiding $P_{WM}(j)$, and also the beginning location (i) of the iris template by the secret key used during the encoding stage. The decoding process is as Eq. (2).

$$S(i) = \begin{cases} P_{WM}^{(1)}(j), & if \quad P_{WM}^{(0)}(j) = 0; \\ \overline{P_{WM}^{(1)}(j)}, & if \quad P_{WM}^{(0)}(j) = 1; \end{cases} \quad (2)$$

Where the reverse of $P_{WM}^{(1)}(j)$ is denoted as $\overline{P_{WM}^{(1)}(j)}$. Finally, every bit $S(i)$ is orderly filled the corresponding location of the iris template $I(k, l)$.

The bit-stream technique has the following aspects:

- The encoding and decoding calculations are just bit's comparison or reversion so the high calculation efficiency is reasonable.
- The decoding error rate is zero.
- The proposed method is not lossless to the host image because the change in the gray value of the pixels in the host image just happens to the lowest bit of each pixel.

- Hiding a target biometric data (iris template) into another biometric data (face image) can deceives attackers more effectively in identity verification, biometric data storage and transmission.
- The hiding process is applied on the transformed iris template not the original iris template.

3. The Proposed Method

However the bit stream technique has many aspects, the computation time of the encoding and decoding depends on the bit length of the iris template data. This problem is solved by our proposed method.

In the encoding stage, starting from the original byte and with number of pixels equal to the number of the bits in iris template, we transform each pixel $P(j)$ into 8 bits $P^{(0)}(j), P^{(1)}(j), \ldots, P^{(7)}(j)$.
Eq. (1) shows that $P_{WM}^{(0)}(j)$ can be obtained by an XOR operation between $S(i)$ and $P^{(1)}(j)$. So we apply parallel XOR operations between each bit $S(i)$ in the iris template $I(k, l)$ and each bit $P^{(1)}(j)$ in the vector $P^{(1)}$ that contains all $P^{(1)}(j)$(starting from the original bit and original byte), respectively. The result of XOR operation is $P_{WM}^{(0)}$, as in Eq. (3).

$$P_{WM}^{(0)} = \text{XOR}\,(I, P^{(1)}) \quad (3)$$

So we are embedding all the bits in the iris template into the face image in one encoding run instead of embedding bit by bit.

In the decoding stage, starting from the original byte and with number of pixels equal to the number of the bits in iris template, we transform each pixel $P_{WM}(j)$ into bits $P_{WM}^{(0)}(j), P^{(1)}(j), \ldots, P^{(7)}(j)$.
Eq. (2) shows that $S(i)$ can be obtained by an XOR operation between $P_{WM}^{(0)}(j)$ and $P_{WM}^{(1)}(j)$. So we apply parallel XOR operations between each bit $P_{WM}^{(0)}(j)$ in the vector $P_{WM}^{(0)}$ that contains all $P_{WM}^{(0)}(j)$ and each bit $P_{WM}^{(1)}(j)$ in the vector $P_{WM}^{(1)}$ that contains all $P_{WM}^{(1)}(j)$ (starting from the original bit and original byte), respectively. The result of XOR operation is $I(k, l)$ as in Eq. (4).

$$I(k, l) = \text{XOR}\,(P_{WM}^{(0)}, P_{WM}^{(1)}) \quad (4)$$

So we are extracting all the bits in the iris template from the face image in one decoding run instead of extracting bit by bit.

4. Experimental Results

4.1 The Databases

In our experimentation, we used two biometric databases. The first database is the BioID Face database [9] which consists of 1,521 face images (8- bit gray level) with a

resolution of 384x286 pixels. Each image has the frontal view of a face for 23 subjects. The second database is the CASIA database [10] for the iris images which consists of 756 iris images (8- bit gray level) with a resolution of 320x280 pixels.

4.2 Extracting Iris Features

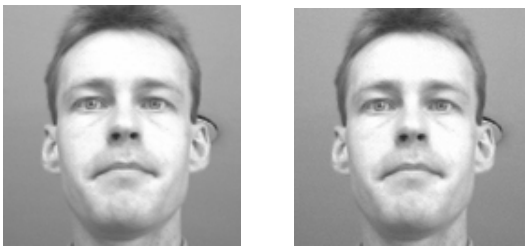
From 100 iris images, the iris templates are calculated according to the method presented in [11].

4.3 The Effect of the Proposed Method on the Performance of the Iris Recognition

The iris template is matched before embedding in the face image using Hamming distance [11]. And also is matched after decoding from the face image. The results are compared. The comparison ensures that the proposed method does not affect on the performance of iris recognition.

4.4 The Effect of the Proposed Method on the Face Image

"Fig. 3(a)" is the original face image and "Fig. 3(b)" is the hidden image. By the visual observation, there is no difference between the two images.



(a) Original face image (b) Image hidden data

Fig. 3 Comparison of data hiding before and after.

4.5 Comparison between the Proposed Method and Bit Stream Method [8]

All the algorithms were implemented in MATLAB 7.0. The 'Time' column of Table 1 contains the average watermarking time using the method in [8] and our proposed method. These time values were obtained by averaging 100 watermarking processes on 100 distinct images.

Table 1: Comparison between the proposed method and bit-stream method

Method	*Time (s)*
The proposed method	3
Bit steam method	57

5. Conclusions

In recent years, with the increased use of biometrics for user authentication, an increase in the demand for the security of the biometric databases has occurred. Public concerns about safety of their biometric templates if the database is compromised as well as fears of cross-referencing among databases had to be addressed to ensure public acceptance of the use of biometric systems in large scale applications. In this paper, we present a scheme for securing revocable iris templates using parallel-bit stream based data hiding method. Experimental results show that the proposed method has low computation time and can availably be used to protect iris feature template data and enhance the self-security of the iris recognition system.

References

[1] Anil K. Jain, Umut Uludag, "Hiding Biometric data", *IEEE Transactions on Pattern Analysis and Machine Intelligence,* Vo1.25, No.ll, November 2003.

[2] Vatsa M., Singh R., Mitra P., Noore A., "Comparing robustness of watermarking algorithms on biometrics data", *Proceedings of the Workshop on Biometric Challenges from Theory to Practice – ICPR Workshop,* pp. 5–8, 2004.

[3] Park K. R., Jeong D. S., Kang B. J., Lee E. C., "A Study on Iris Feature Watermarking on Face Data", *ICANNGA(2),* pp. 415-423, 2007.

[4] Marwa Fouad, Abdulmotaleb El Saddik, Emil Petriu, "COMBINING DWT AND LSB WATERMARKING TO SECURE REVOCABLE IRIS TEMPLATES", 2009.

[5] Ratha, N. and Connell, J., "Cancelable Biometrics", *presented at Biometric Consortium 2000 Conference*, Sept. 13-14, 2000.

[6] S. Kanade, D. Camara, E. Krichen, D. Petrovska-Delacretaz, B. Dorizzi, "Three factor scheme for biometric-based cryptographic key regeneration using iris", *Biometrics Symposium, BSYM '08,* pp: 59-64, 23-25 Sept. 2008.

[7] J. Zuo, N.K. Ratha, J.H. Connell, "Cancelable iris biometric", 19th International Conference on Pattern Recognition *(ICPR), pp*.1-4, December 2008.

[8] Ye X., He Z., and Zhang W., "A data hiding method for improving the self-security of iris recognition", *International Conference on Communications, Circuits and Systems, ICCCAS,* pp. 762-766, May 2008.

[9] BioID Face DB of Humanscan Corp., http://humanscan.de/support/downloads/facedb.php (accessed on 15 January 2012).

[10] CASIA iris DB of Chinese AcademyofScience,http://www.sinobiometrics.com/ resources.htm (accessed on 15 January 2012).

[11] John Daugman, "How Iris Recognition Works", *IEEE Transactions on circuits and systems for video technology,* Vol. 14, No.1, Jan.2004