Prof. Mrs. Neha Hajare, Anuja Borage, Nikhita Kamble, Supriya Shinde / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 2, March -April 2013, pp.1320-1323

Biometric Template Security Using Visual Cryptography

Prof. Mrs. Neha Hajare, Anuja Borage, Nikhita Kamble, Supriya Shinde
(Faculty of Computer Engineering, MIT Academy of Engineering, Alandi, Maharashtra, India)
(Department of Computer Engineering, MIT Academy of Engineering, Alandi, Maharashtra, India)

ABSTRACT

Biometrics deal with recognizing a person or verifying the identity of a person based on physiological or behavioral characteristics. Visual cryptography is a secret sharing scheme where a secret image is encrypted into the number of shares which independently disclose no information about the original image. There are various biometric templates like fingerprints, face, voice, signature, iris and odor. Amongst all these templates, the iris template is the most universal, unique and permanent. Also, its performance is comparatively higher than the other templates. So we are focusing on iris template. The previous work involved storing of original template in the system which was vulnerable to various attacks, but in our proposed work, we are storing the extracted image of the template. Also, we are assigning a unique number to every template which is encrypted using Visual Cryptography. Visual cryptography provides an extra layer of authentication. The combination of biometrics and visual cryptography is a promising information security technique which offers an efficient way to protect the biometric template. In this work, we are providing two fold security to the iris template.

Keywords– **Authentication, Biometric Template, Iris, Visual Cryptography.**

1. INTRODUCTION

Security of data has been a major issue from many years. Using the age old technique of encryption and decryption has been easy to track for people around. Providing security to data using new technique is the need of the hour. This project uses the technique of Visual cryptography and providing biometric authentication.

For automated personal identification biometric authentication is getting more attention [1]. Biometrics is the detailed measurement of human body. Biometrics deal with automated methods of identifying a person or verifying the identity of person based on physiological or behavioral characteristics. There are various applications where personal identification is required such as passport. Controls, computer login control, secure electronic banking, bank ATM, credit cards, airport, mobile phones, health and social services, etc. Many biometric techniques are available such as facial thermogram, hand vein, odor, ear, hand geometry, fingerprint, face, retina, iris, palm print, voice and signature. Among those iris recognition is one of the most promising approach because of stability, uniqueness and noninvasiveness [2].

There are certain issues related to biometric system and biometric data. Biometric systems are vulnerable to attacks, which can decrease their security [3]. As template is stored in database, if the security of stored templates is compromised, the attacker can gain unauthorized access. The stolen templates can also be used for other unintended purposes, e.g. performing unauthorized credit-card transactions or accessing health related records. Hence, biometric templates should not be stored in plaintext form and fool-proof methodologies are essentially needed to securely store the templates. We can protect the biometric data and template by using cryptography, steganography and watermarking. In this paper a system is proposed by visual cryptography technique to protect the iris template to make it secure from attack in system database as well as dual layer of authentication to the users.

2. RELATED WORK

2.1. Biometric template attacks

Biometrics is the detailed measurements of the human body. A brief comparison of nine biometric techniques made by A. Jain et al. in 1997 is provided in Table 1 below.

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance
Face	High	Low	Medium	High	Low
Fingerprint	Medium	High	High	Medium	High
Iris	High	High	High	Medium	High
Signature	Low	Low	Low	High	Low
Voice	Medium	Low	Low	Medium	Low

Table 1. Comparison of biometric technologies

Now-a-days, recognizing person using alphanumeric passwords is not sufficient for the identity determination because they can be easily guessed or stolen. Therefore using biometric system is generally pattern recognition system that determines person based on his physiological characteristic. Use of the biometric templates provides advantages like convenience, reliability, universality etc. Several places where attacks are

possible in biometric system are shown in Fig. 1 below.

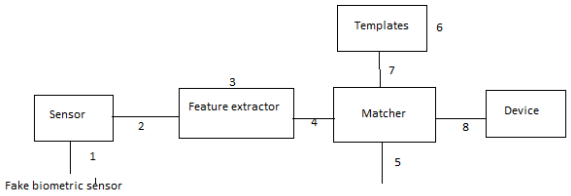


Figure 1. Attacks

2.2. Visual Cryptography

The basic visual cryptography scheme was proposed by Naor and Shamir's[4] .In this scheme for sharing a single Pixel p, in a binary image Z into two shares A and B is illustrated in Table I. If p is white, one of the first two rows of Table 1 is chosen randomly to encode A and B. If p is black, one of the last two rows in Table I is chosen randomly to encode A and B. Thus, neither A nor B exposes any clue about the binary color of p. When these two shares are superimposed together, two black sub-pixels appear if p is black, while one black sub-pixel and one white

sub-pixel appear if p is white as indicated in the rightmost column in Table 1. Based upon the contrast

between two kinds of reconstructed pixels can tell whether p is black or white. Performance of visual cryptography scheme mainly depends on pixel expansion and contrast. Pixel expansion refers to the number of subpixels in the generated shares that represents a pixel of the original input image. It represents the loss in resolution from the original picture to the shared one. Contrast is the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original image. Plenty of research has been made to improve the performance of basic visual cryptography scheme. Many authors have proposed the visual cryptography schemes in which pixel expansion is 1 [5, 6]. These schemes can be used as quality of retrieved images is good.

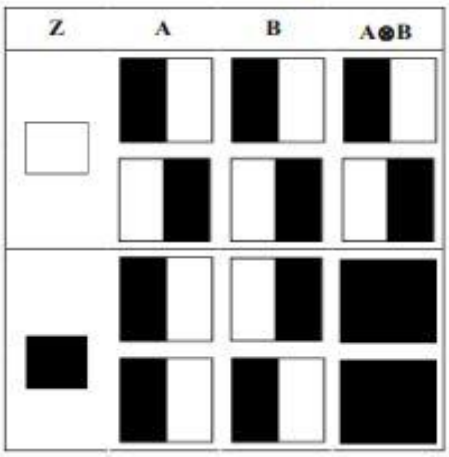


Figure 2. Visual Cryptography

3. PROPOSED SYSTEM

Since, securing the iris template is the main aim of our project we are using Visual Cryptography technique for protecting the iris template. In this system there are two main modules: Enrollment module and Authentication module. Enrollment module is further divided into two sub modules namely: SNF module and VC module. If we consider an example of an employee working in an organization, he will have to go through both the processes given below to have access to his organization.

3.1 Enrollment

There are two sub modules: SNF module and VC module.

3.1.1 SNF Module

The system administrator will collect the eye image of the employees for letting them access to the organization. These images will be given to the SNF module which includes three steps that are: Segmentation, Normalization and Feature extraction. From this, the extracted iris template is stored in the database with name as any random number. Further, the bmp/png image of this number will be made and sent to the VC module. The three steps of the SNF module are explained below [13].

Segmentation: This is performed to extract the iris template from the eye image. The Hough Transform, a standard computer vision algorithm is used here to deduce the radius and centre coordinates of the pupil and iris region. The circular Hough Transform algorithm is employed by Wildes et al. [7], Kong and Zhang [8],Tisse et al. [9], and Ma et al. [10] in which eyelids are detected and eyelash is separated by threshold technique.

Normalization: This is performed to remap each pixel within the iris region to a pair of polar coordinates. It is carried out using the Daugman's rubber sheet model. Here, the centre of the pupil is considered as the reference point and the radial vectors circle through the iris region. Another point of note is that the pupil region is not always concentric within the

iris region, and is usually slightly nasal [11]. This must be taken into account if trying to normalize the 'doughnut' shaped iris region to have constant radius.
Feature Extraction: In order to provide accurate recognition of individuals, the most discriminating information present in an iris pattern must be extracted. Only the significant features of the iris must be encoded so that comparisons between templates can be made. This is done by convolving the normalized iris pattern into Gabor Filters. The resulting phase information for both the real and imaginary response is quantized.

3.1.2 VC Module

The extracted iris template is stored in the database and using Random number generator algorithm, a random number is generated and is stored in the database as the extracted template image's name. This number is given as input to the VC module which then generates two shares, out of which one share is stored in the database and the other is stored on the user ID card. This ends the enrollment module.

3.2 Authentication

For this phase, user will come and give his eye image. His eye image will go through the SNF process. Then this extracted image will be compared with the extracted image stored in the database while enrollment phase. If both the templates match then we consider that the user is a registered employee and he can proceed for the further Login process. But, if the templates do not match, then the user is asked to go through the enrollment phase.

Once he proceeds to the Login process, he will provide the ID card on which the share is stored. At the same time system will find his corresponding second share from the database. These both shares will be superimposed and will be decrypted to find the number. The decrypted number will be compared with the image name which was also stored as the number. If both the numbers match then the user is given access to the organization. But, if they don't match then access is denied. Here, there may be a possibility of the user being a registered employee of the organization but the card which he is using does not belong to him. So even if the extracted templates match in the first process of authentication, because of the two fold security, the stolen ID card can be returned to the employee who owns it.

The working of proposed system is shown in Fig. 3 and 4 below.

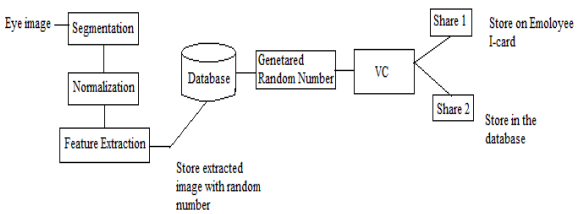


Figure 3. Employee Enrollment

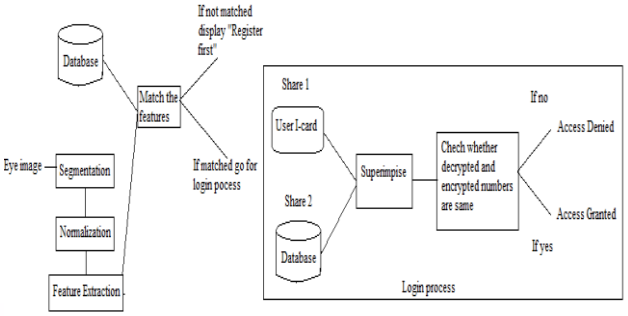
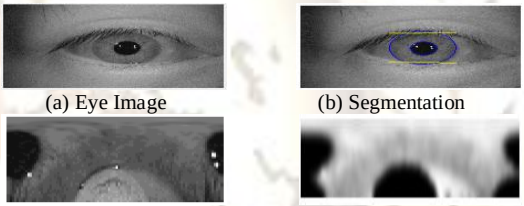


Figure 4. Employee Authentication

4. EXPERIMENTS AND RESULTS

To build this system, previously MATLAB platform was used. But we have implemented it using JAVA platform since security is one of the buzzwords of JAVA. Iris images are taken from The Chinese Academy of Sciences - Institute of Automation (CASIA) eye image database [12] contains 756 grayscale eye images with 108 unique eyes or classes and 7 different images of each unique eye.



(a) Eye Image (b) Segmentation

(c) Normalization (d) Feature Extraction

Figure 5. Results of SNF module

5. CONCLUSION AND FUTURE WORK

There are various techniques adopted by the researchers to secure the raw biometric templates. In this paper a method is proposed to provide two-fold security to the iris template using Visual Cryptography.

ACKNOWLEDGEMENTS

We express our gratitude to Mrs. Uma Nagaraj, Head of the Department and our Guide Mrs. Neha Hajare for providing us the adequate facilities, ways and means by which we were able to complete this paper. We would also like to thank Research coordinator Mr. Piyush Deolikar, for his support and faith in us. We thank them all for their constant support and valuable suggestions without which the successful completion of this paper would not have been possible.

REFERENCES

Journal Papers:

[1] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric recognition: security and privacy

concerns".In Proceedings of the *IEEE Security & Privacy,33-42,* March/April 2003.

[2] J. Daugman, "High confidence recognition of persons by test of statistical independence".*IEEE Trans. on PAMI, vol. 15,1148-1160,*1993.

[3] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle, "An Analysis of Minutiae Matching Strength". In Proceedings of *the 3rd AVBPA, Halmstad, Sweden,223-228* ,June 2001.

[4] Moni Naor and Adi Shamir, "Visual cryptography" .In Proceedings of the *advances in cryptology– Eurocrypt, 1-12,*1995.

[5] Lin Kezheng, Fan Bo, Zhao Hong, "visual cryptographic scheme with high image quality". In Proceedings of *the International Conference on Computational Intelligence and Security, 366-370,IEEE* ,2008.

[6] Xiao-qing Tan, "Two kinds of ideal contrast visual cryptography schemes". In Proceedings of the *International Conference on Signal Processing Systems, 450-453, 2009.*

[7] Jing Dong, Tieniu Tan, "Effects of watermarking on iris recognition performance". *978–1–4244–2287–6,IEEE,* 2008.

[8] Wen-Pinn Fang "Non-expansion visual secret sharing in reversible style". *IJCSNS International Journal of Computer Science and Network Security, 9(2),* February 2009.

[9] H.-C. Hsu, T.-S. Chen, Y.-H. Lin, "The ring shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing". In Proceedings of the 2004 *IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, pp. 996–1001,* March 2004.

[10] Xiao-qing Tan, "Two kinds of ideal contrast visual cryptography schemes". In Proceedings of the *International Conference on Signal Processing Systems, 450-453,* 2009

[11] A. Juels and M. Wattenberg, "A fuzzy commitment scheme". In Proceedings of the *6th ACM conference on Computer and communications security. New York, NY, USA: ACM Press, 28–36,*1999.

[12] Lin Kezheng, Fan Bo, Zhao Hong, "visual cryptographic scheme with high image quality". In Proceedings of the *International Conference on Computational Intelligence and Security, 366-370,IEEE* ,2008.

Theses:

[13] Libor Masek "Recognition of Human Iris Patterns for Biometric Identification "