

Secure Iris Recognition with Visual Cryptography

Sheetal Chaudhary¹, Rajender Nath² and Chander Kant³

^{1,2,3}*Department of Computer Science & Applications, Kurukshetra University,
Kurukshetra, India*

¹*sheetalkuk@rediffmail.com, ²math_2k3@rediffmail.com,*

³*ckverma@rediffmail.com*

Abstract

Biometrics is the science of uniquely recognizing an individual based on his/her physiological or behavioral characteristics. Amongst all the biometric characteristics, iris recognition is the most secure technique due to its stability and uniqueness. In this paper, an approach based on visual cryptography has been proposed to protect the biometric template of iris. Visual cryptography is a secret sharing technique which divides the secret image into number of shares which independently reveals no information about the original image. It is impossible to obtain any information about the secret image from shares individually. It does decryption simply by human visual system without any cryptographic computations. Experimental work has been performed on a public dataset to demonstrate the performance of proposed approach and it seems an efficient way to protect the biometric template.

Keywords: *Security, biometric template, visual cryptography, iris, secret sharing*

1. Introduction

Biometric characteristics are inherent features of the person to be authenticated that's why biometrics is getting more attention for automated personal identification. It requires no password to remember and no ID card to carry along. Generally, a biometric recognition system works by acquiring raw biometric data from various biometric characteristics (iris, face image, fingerprint, hand geometry, gait, signature *etc.*) that are possessed by the person to be authenticated. Relevant feature set is extracted from the acquired data and it is compared against the templates stored in the database with the aim of identifying the person or to verify the claimed identity [1].

The biometric systems are vulnerable to numerous attacks which declines their security. Attacks on biometric systems have been analyzed and classified into eight types [2]. A typical biometric system with these attack points is shown in Figure 1. Type 1 attack is providing a fake biometric characteristic to the sensor module. Type 2 attack is submitting previously captured biometric data to the system. In type 3 attack, the feature extraction module is forced to generate feature sets that are chosen by attacker. In type 4 attack, genuine feature sets are replaced with those selected by the attacker. Type 5 attack is on the matcher module which is modified to produce a falsely high matching score. Type 6 attack is on the template database. In type 7 attack, the transmission medium between template database and matcher module is attacked which results in modification of the send out templates. Type 8 attack is to override the result *i.e.*, accept or reject given by the decision module.

Received (May 16, 2018), Review Result (July 17, 2018), Accepted (August 22, 2018)

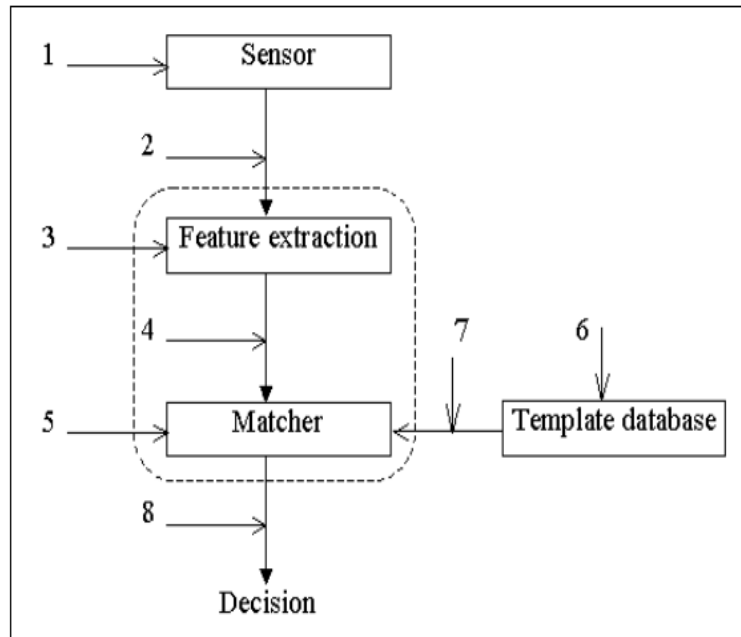


Figure 1. Attack Points in a Biometric System

Among these attacks, the most damaging attack is on the template database. Though biometrics provides an acceptable form of security but depending exclusively on that can be unsafe. Thus, it has necessitated the need to make templates secure by protecting the contents of the database with the help of some powerful techniques. Due to vulnerability to various types of attacks [2], biometrics is not safe as a primary authenticator. If it is merged or used along with other security methods (such as steganography, watermarking, cancelable biometrics *etc.*) then they will provide an extra layer of security to biometric information stored in databases. In this paper, visual cryptography technique is used to protect the iris template and to keep it safe from attacks in system database. The basic process of visual cryptography is illustrated in Figure 2.

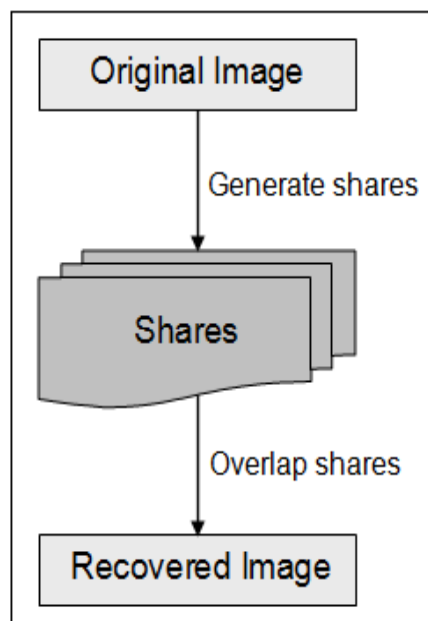


Figure 2. Basic Process of Visual Cryptography

The fundamental concept of visual cryptography was proposed by Naor and Shamir [3]. It is a cryptographic technique which allows encryption of visual information (text, images *etc.*) in such a way that their decryption can be carried out without any cryptographic algorithm. The decryption is performed simply by human visual system. It divides the visual information into number of images where each image is a collection of black and white pixels. Each of the images is termed as a secret share. No information about the original image can be obtained from these secret shares individually. Each pixel of the original image is represented by some fixed number of pixels in each share. There are various types of visual cryptography schemes (VCS) *e.g.*, k -out-of- n [3], for gray level images [4], halftone [5], for color images [6], extended visual cryptography for natural images [7], progressive [8], for general access structures [9] *etc.*

Visual cryptography can be accomplished by using any one of the following access structure schemes [3]. In this paper, 2-out-of-2 *i.e.*, (2,2) visual cryptography scheme is used.

- (2,2) Threshold VC Scheme — This is the simplest threshold scheme that divides the secret image in two different shares such that the secret image is exposed when these two shares are overlaid.
- (2, n) Threshold VC Scheme — This scheme divides the secret image into n shares such that when any two (or more) of the shares are overlaid the secret image gets exposed.
- (n , n) Threshold VC Scheme — This scheme divides the secret image into n shares such that when all n of the shares are overlaid the secret image gets exposed.
- (k , n) Threshold VC Scheme — This scheme divides the secret image into n shares such that when only k or more than k number of shares are overlaid the secret image will be exposed. Less than k number of shares can't recover the original information.

This paper is organized as follows. Related works for visual cryptography schemes are discussed in Section 2. Section 3 describes the proposed work. Experimental work is demonstrated in Section 4 and Section 5 concludes the paper.

2. Related Work

This section gives a brief introduction of works related with visual cryptography and its applications. Visual Cryptography has become increasingly popular in the last some years. The fundamental visual cryptography method was introduced by Naor and Shamir [3].

A visual cryptographic technique has been applied to feature sets of fingerprint wherein a construction of a blind alignment of the fresh image and the reference image was proposed [10]. Based on the visual cryptographic scheme, fingerprint image was divided into two shares and these shares were stored in separate databases.

A biometric system for protecting the face image using visual cryptographic scheme was proposed wherein secret image was broken into two shares [11]. It was not easy to recognize the secret image with one share. It could be discovered only when both the shares were presented at the same time.

A three-step hybrid approach that effectively used the advantages of cryptosystems as well as cancelable biometrics was proposed [12].

A fingerprint biometric system based on visual cryptography scheme to resolve the authentication issues was proposed wherein fingerprint image was divided into two shares [13]. One of the shares was stored in the bank database and other one was given to the

customer. Hash code has been created for each customer share to be stored in the bank database. During the transaction, the customer gives one share and this share was combined with the other share that was stored in the database. This improves the security level for authentication in biometrics.

A face swapping method which protected the characteristics of a face image by automatically substituting it with alternate images taken from a public library of face images was proposed [14].

A scheme based on visual cryptography that could be applied only for printed text or image was proposed wherein transparencies were used to print shares [15].

A visual cryptography method based on random basis column pixel expansion technique was proposed [16]. The encoded shares were further encoded into number of sub shares recursively which was computationally complex.

3. Proposed Work

Based upon the literature survey, it is clear that biometric systems are at risk of various attacks. Among these attacks, an attack upon the templates in biometric databases is most dangerous because biometric templates uniquely define a person's identity and are irrevocable in nature. Biometric characteristics used to generate templates are personal features of the persons who possess them. If this personal data is stolen or copied by unauthorized persons, it is impossible to replace it. The misuse of templates leads to a number of security and privacy issues such as a genuine template can be substituted with an imposter's template in database, the stolen template can be submitted directly to the matcher module again and again, loss of privacy as the same template could be used to access multiple services. To solve the issues related with template security in biometric databases, an approach based on visual cryptography has been presented in this paper. Here, both left iris and right iris are used as input biometric traits. This approach stores only part of template in database and the rest is kept at user's ID. This makes original template secure by not allowing unauthorized or imposter person to access the full template. The imposter person would no longer be able to use the facilities meant only for legitimate person with this incomplete template.

3.1. Feature Set Extraction of Iris

Iris is the colored portion of an eye that controls the size of pupil. It is an annular region between the pupil and white portion of the eye *i.e.*, sclera. It consists of many features such as coronas, freckles, furrows, stripes, crypts etc. These features are unique to each individual and thus make iris a distinct and reliable physical characteristic.

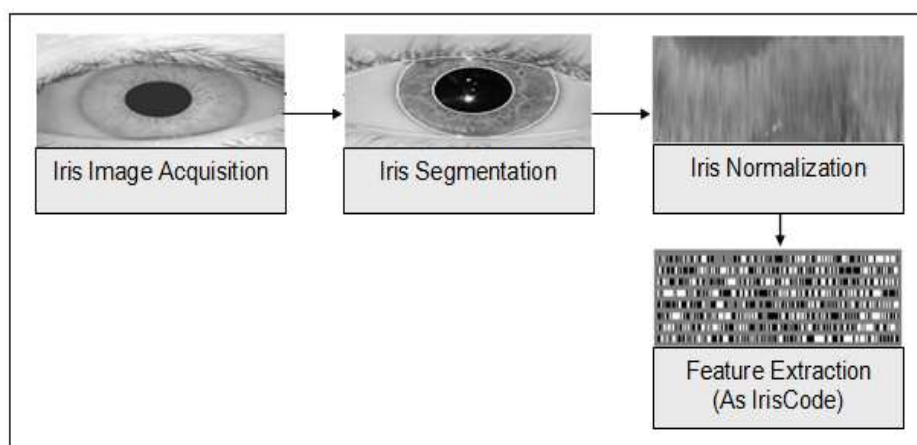


Figure 3. Iris Feature Set Extraction

The basic steps of iris feature set extraction are shown in Figure 3. Preprocessing of original image is done so that iris features could be extracted from it. It consists of segmentation and normalization of the iris image. Segmentation is the process of locating iris region in the original image. It recognizes the inner and outer boundaries of iris (*i.e.*, pupil boundary and iris boundary) and also removes the eyelashes of eyelids covering the iris region. The Circular Hough Transform (CHT) is used to recognize these two circles [17]. Iris normalization is carried out with the help of Daugman's rubber sheet model [18] that converts an iris image from Cartesian coordinates to polar coordinates. The resulting normalized iris image is a rectangular image with angular and radial resolutions. It eliminates the dimensional inconsistencies that occur due to variation in illumination, distance from camera, size of pupil etc. while capturing the image of an eye. Gabor filter with 2D Gaussian function [19] is used to extract the features of iris from normalized iris image. Feature set is obtained in the form of an iris code which is the unique 2048 bit representation of iris image.

3.2. Fusion at Feature Level

Feature level fusion is the consolidation of feature sets or templates related to two or more than two biometric characteristics. Let I_L and I_R represent the feature sets extracted from the images of left and right irises respectively. These two feature sets are integrated to perform fusion at feature level. It creates a new fused iris template *i.e.*, I_{Iris} that better represents the both individual feature sets. To generate I_{Iris} , the two feature sets (*i.e.*, left and right irises) are first concatenated and then feature selection process is applied on the resulting fused feature set to reduce its dimensionality and produce a minimal or optimal feature set.


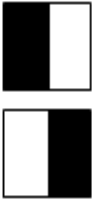
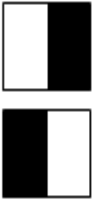


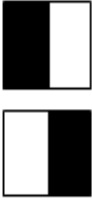
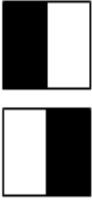
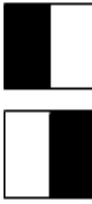
$$I_{Iris} = I_L + I_R \quad (1)$$

3.3. Visual Cryptography

Visual Cryptography is an absolutely secure method for protection of secret images. It is a cryptographic technique which performs encryption by dividing the secret image into random shares and performs decryption by superimposing the shares. One of its advantages is that it does not need any special software or hardware for doing cryptographic calculations and it is simply impossible to obtain any information about the secret image from shares individually. The visual cryptography scheme (VCS) has been introduced by Naor and Shamir [3] and can be applied by any one of the four access structures *i.e.*, 2-out-of-2, 2-out-of-n, n-out-of-n, and k-out-of-n. They also assumed that in a share white pixel (which is represented by binary 0) is considered as transparent and black pixel (which is represented by binary 1) is considered as opaque.

In proposed approach, 2-out-of-2 Visual cryptography scheme with two subpixels is used as represented in Table 1. It divides each pixel of secret image (*i.e.*, fused iris template) into two shares (share 1 and share 2). Representation of different types of shares is shown in Figure 4. If pixel is black, one of the first two rows in Table 1 can be selected arbitrarily to encode share 1 and share 2. If pixel is white, one of the last two rows in Table 1 can be selected arbitrarily to encode share 1 and share 2. Here, each pixel is divided into four subpixels such that each share is composed of one white and one black pixel. Individual share reveals no information whether a particular pixel is white or black so it is impossible to decrypt the shares. The original pixel is recovered by simply stacking or superimposing the two shares together. It is equivalent to using the OR operation between the shares. The stacking or superimposing of two shares (*i.e.*, share1 + share 2) is depicted in last column of Table 1. It will consist of two black subpixels if original pixel is black and consist of one black subpixel and one white subpixel if original pixel is white.

Table 1. 2-Out-Of-2 Visual Cryptography Scheme with 2 Subpixels

Original Pixel	Share 1	Share 2	Share 1 + Share 2
 Black			
 White			

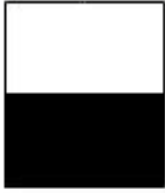
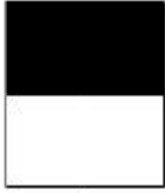
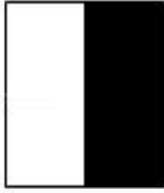

			
Horizontal shares (a)		Vertical shares (b)	

Figure 4. Types of Shares (a) Horizontal (b) Vertical

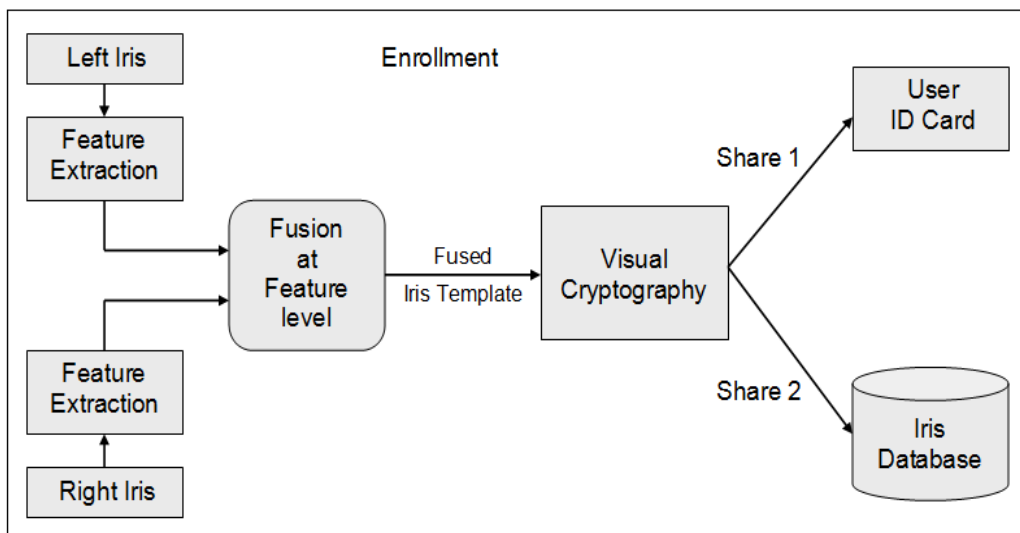


Figure 5. Enrollment Process of Proposed Approach

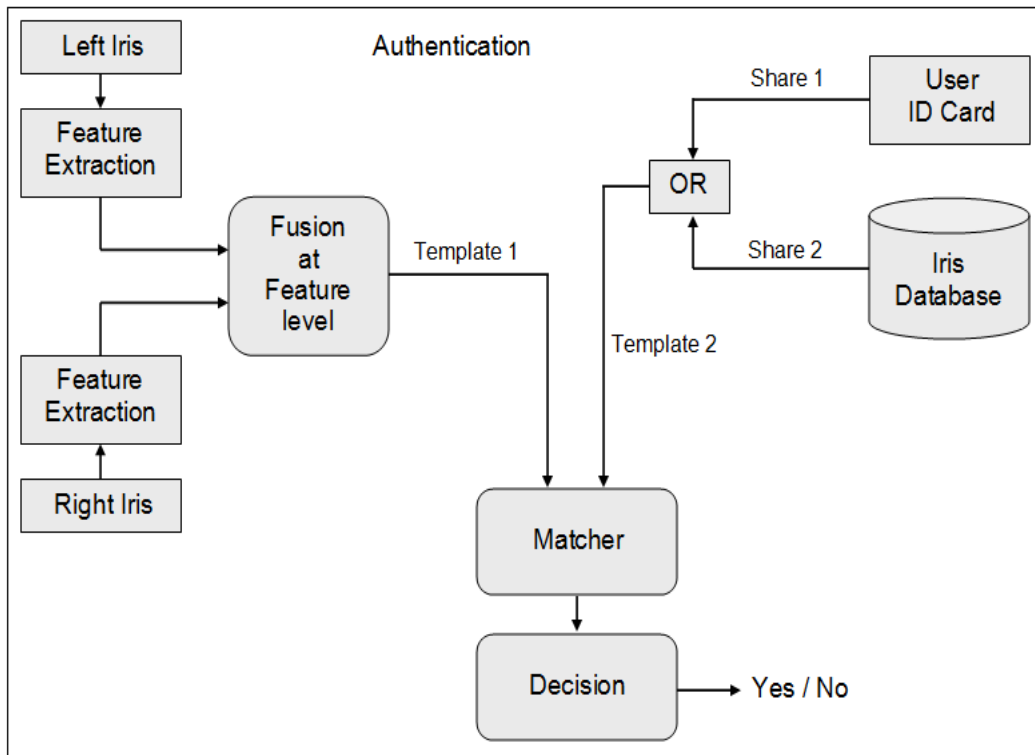


Figure 6. Authentication Process of Proposed Approach

3.4. Proposed Algorithms

The architecture of proposed approach consists of two processes *i.e.*, enrollment and authentication as shown in Figures 5 & 6. The proposed algorithms for both processes are discussed below:

Algorithm: Enrollment Process

Begin

1. Capture images of left and right irises with the help of a suitable sensor.
2. Generate templates or salient features of both left and right irises.
 - a) Segmentation
 - b) Normalization
 - c) Feature set extraction
3. Perform fusion of left and right irises at feature level to generate a single fused iris template.
 - a) Check the compatibility of feature sets to be combined
 - b) Normalization
 - c) Feature selection
4. Apply visual cryptography on fused iris template to generate two shares *i.e.*, share 1 and share 2.
5. Store share 1 in user ID card and share 2 in iris database.

End

Algorithm: Authentication Process

Begin

1. Capture images of left and right irises with the help of a suitable sensor.
2. Generate templates or salient features of both left and right irises.
 - a) Segmentation

- b) Normalization
 - c) Feature set extraction
 3. Perform fusion of left and right irises at feature level to generate a single fused iris template.
 - a) Check the compatibility of feature sets to be combined
 - b) Normalization
 - c) Feature selection
 4. Generate the enrolled template by doing logical OR of share 1 (obtained from user ID card) and share 2 (obtained from iris database).
 5. Perform matching of current template (generated in step 3) with the enrolled template (recreated in step 4).
 6. If (match score > threshold)
 User is authenticated.
 Else
 User is rejected or not authenticated.
- End

4. Results and Discussion

Visual cryptography has two important features. The first feature is its perfect secrecy and the second feature is its decryption method which requires neither complex decryption algorithms nor the help of computers. It utilizes only human visual system to recreate the original image from the stacked set of shares. It also preserves the privacy and integrity of biometric data as the original image is recovered only when both shares are available simultaneously. It minimizes the cost of storing biometric templates as only one share is stored in the database.

4.1. Database

The sample images of iris used in the proposed approach are taken from CASIA [20] database. Figure 7 shows the sample images of left iris and right iris.

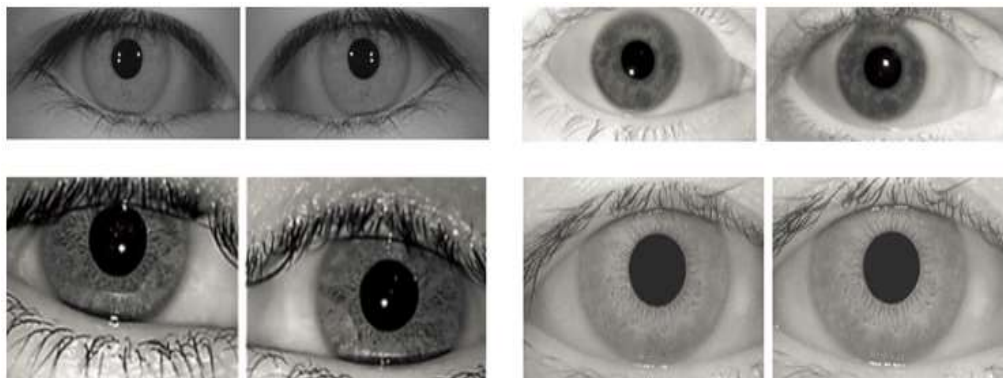


Figure 7. Sample Images of Left Iris and Right Iris

4.2. Performance Evaluation

This section demonstrates the performance of proposed approach on the basis of the results obtained after doing experimental evaluations on a public dataset. MATLAB is used for evaluating its performance. Here, 2-out-of-2 visual cryptography technique is applied on iris template. Figure 8(a) shows original iris template image, 8(b) and 8(c) shows share 1 and share 2, and 8(d) shows image generated after superimposing share 1 and share 2. The two shares individually do not expose any useful information about iris template. The spatial arrangement of pixels in these shares varies from block to block.

Hence, it is essential to access both the shares simultaneously to recover the original template. The OR operator is used to superimpose the two shares to retrieve the original template. Here, authentication is achieved by matching the current template with secret template that is obtained after superimposing the shares derived using the visual cryptography algorithm. The performance of proposed approach does not degrade when the original template is recovered by stacking the corresponding shares.

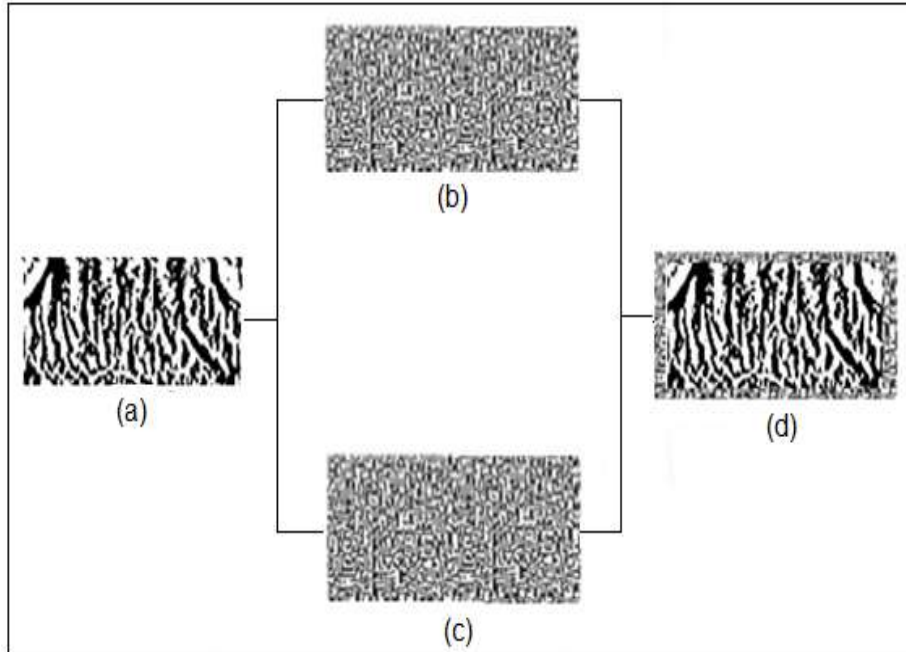


Figure 8. (a) Iris Template Image (b) Share 1 (c) Share 2 (d) Image obtained after Superimposing share1 and share 2

In general, the performance of a biometric recognition system is calculated by False Acceptance Rate (FAR) and False Rejection Rate (FRR) [21]. FAR and FRR are computed as follows:

$$\text{FAR (\%)} = \frac{\text{false acceptance numbers}}{\text{number of wrong matches}} \times 100\% \quad (2)$$

$$\text{FRR (\%)} = \frac{\text{false rejection numbers}}{\text{number of correct matches}} \times 100\% \quad (3)$$

The Receiver Operating Characteristic (ROC) curve in Figure 9 shows the performance of proposed approach at different threshold values. The Equal Error Rate (EER) is the point at which FAR and FRR are equal. The value at this point indicates that the proportion of false acceptances is equal to the proportion of false rejections. The performance of biometric system is better if value of EER is lower or near to 0%. It is clear from ROC curve that the proposed system shows good recognition performance at EER 2.3%.

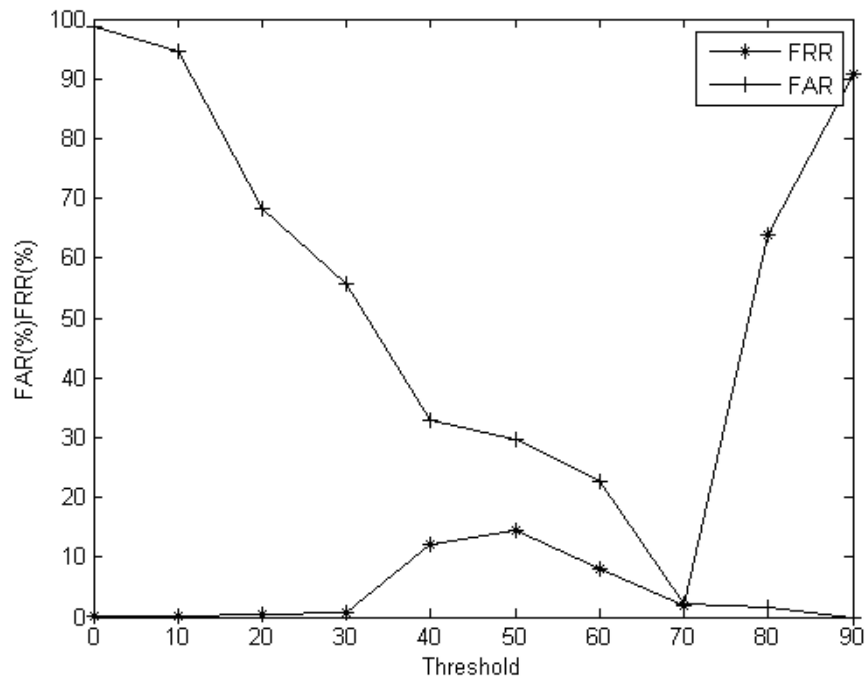


Figure 9. ROC Curve Showing Error Rates at Various Thresholds

5. Conclusion

To prevent biometric systems from being susceptible to several attacks, it is important to protect and secure biometric templates in the database. In this paper, an approach has been proposed to protect iris template in the database using visual cryptography. It is a secret sharing scheme which splits the secret image into n shares and recovers it by superimposing the enough shares. Any information about the secret image can't be retrieved from individual shares. The other advantage is that, it does not need any cryptographic calculations to recover the secret image unlike other cryptography techniques. Rather, it uses human visual system to reveal the original image. Experimental results show that the matching performance of iris recognition system remains unaffected with this extra layer of authentication. Thus, it is a simple and secure method to protect templates in database. Though this approach is presented for iris recognition system, it can be easily applied to other biometric characteristics also.

References

- [1] N. Ratha, J. Connell and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM System Journal, vol. 40, no. 3, (2001), pp. 614-634.
- [2] N. K. Ratha, J. H. Connell and R. M. Bolle, "An Analysis of Minutiae Matching Strength", In Proceedings of the 3rd AVBPA, Halmstad, Sweden, (2001) June, pp. 223-228.
- [3] M. Naor and A. Shamir, "Visual cryptography", In Proceedings of the Advances in Cryptology–Eurocrypt '94, Lecture Notes in Computer Science, vol. 950, (1995), pp. 1-12.
- [4] C.-C. Lin and W.-H. Tsai, "Secret image sharing with steganography and authentication", The Journal of Systems and Software, vol. 73, no. 3, pp. 405-414, (2004) November-December.
- [5] Z. Zhou, G. R Arce and G. Di Crescenzo, "Half-tone Visual Cryptography", Proc. of IEEE International Conference on Image Processing, Barcelona, Spain, vol. 1, (2003) September, pp. 521-524.
- [6] F. Liu, C. K. Wu and X.J. Lin, "Colour visual cryptography schemes", IET Information security, vol. 2, no. 4, (2008) December, pp. 151-165.
- [7] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images", J. WSCG, vol. 10, no. 2, (2002), pp. 303-310.

- [8] Young-Chang Hou, Zen-Yu Quan, "Progressive Visual Cryptography With Unexpanded Shares", IEEE Transactions on Circuits and Systems for Video Technology, Volume: 21, Issue: 11, pp. 1760 – 1764, Nov. 2011.
- [9] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures", Information and computation, vol. 129, no. 2, (1996) September, pp. 86-106.
- [10] J. Binger and H. Champanne, "Visual Cryptography Applied to Fingerprint Features as a Solution for Prealignment", International Journal of Research Studies in Computer Science and Engineering, vol. 1, no. 4, (2013), pp. 46-52.
- [11] A. Ross and A. Othman, "Visual Cryptography for Biometric Privacy", IEEE Transactions on Information Forensics and Security, vol. 6, no. 1, (2011), pp. 70-80.
- [12] Y. Feng, P. Yuen and A. Jain, "A hybrid approach for face template protection", Proc. SPIE Conf. Biometric Technology for Human Identification, Orlando, FL, vol. 6944, (2008).
- [13] A. Vinodhini, M. Premanand and M. Natrajan, "Visual Cryptography using Two Factor Biometric System for Trust Worthy Authentication", International Journal of Scientific and Research Publications, vol. 3, no. 3, (2012), pp. 1-5.
- [14] D. Bitouk, N. Kumar, S. Dhillon, P. Belhumeur and S. K. Nayar, "Face swapping: Automatically replacing faces in photographs", ACM Trans. Graph., vol. 27, no. 3, (2008), pp. 1-8.
- [15] W.-Q. Yan, D. Jin and M. S. Kananahalli, "Visual Cryptography for Print and Scan Applications", IEEE Transactions, ISCAS-2004, (2004), pp. 572-575.
- [16] T. Monoth and A. P. Babu, "Recursive Visual Cryptography Using Random Basis Column Pixel Expansion", in Proceedings of IEEE International Conference on Information Technology, (2007), pp. 41-43.
- [17] J. Illingworth and J. Kittler, "A Survey of the Hough Transform", in Computer Vision, Graphics, and Image Processing, vol. 44, no. 1, (1988), pp. 87-116.
- [18] J. Daugman, "How iris recognition works", IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, (2004), pp. 21-30.
- [19] A. Manisha Baban and S. Vikhe Pratap, "Iris recognition system using 2D log-gabor filter", International Journal on Advanced Computer Theory and Engineering, vol. 1, no. 2, (2012), pp. 59-62.
- [20] Chinese Academy of Sciences. Center of Biometrics and Security Research. Database of Eye Images. Available from: www.cbsr.ia.ac.cn/IrisDatabase.htm.
- [21] A. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, (2004), pp. 4-20.

