A Novel Retina based Biometric Privacy using Visual Cryptography

M. Suganya[1] **and K. Krishnakumari**[2]

[1]Research Scholar, Department of Computer Science, Rathnavel Subramaniam College of Arts & Science, Sulur, India.
[2]Director, Department of MCA, Rathnavel Subramaniam College of Arts & Science, Sulur, India.

ABSTRACT
Biometrics deal with automated methods of identifying a person or verifying the identity of a person based on physiological or behavioral characteristics. Preserving the biometric privacy such as digital biometric data (eg. face, iris, retina and fingerprint) is very important nowadays. The retinal biometrics is considered one of the most accurate and robust methods of the identity verification. The unique retina features of an individual can be presented in a compact binary form which can be easily compared with the reference template to confirm identity. As biometric template are stored in the centralized database, due to security threats biometric template may be modified by attacker. If biometric template is altered authorized user will not be allowed to access the resource. To deal this issue visual cryptography schemes can be applied to secure the iris template. Visual cryptography is a secret sharing scheme where a secret image is encrypted into the shares which independently disclose no information about the original secret image. The combination of biometrics and visual cryptography is a promising information security technique which offers an efficient way to protect the biometric template. Visual cryptography provides great means for helping such security needs as well as extra layer of authentication.

Keywords:
Biometric, Visual cryptography, Retina authentication, Enrollment, Authentication

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. 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 thermo gram, hand vein, odor, ear, hand geometry, fingerprint, face, retina, iris, palm print, voice and signature. Among those retina recognition is one of the most promising approach because of stability, uniqueness and noninvasiveness.

Biometrics systems are more consistent and more user friendly. Still there are certain issues particularly the security facet of both biometric system and biometric data. As template is stored in centralized database, they are vulnerable to eavesdropping and attacks. Thus alternative protection mechanisms need to be considered. For these reasons various researches have been made to protect the biometric data and template in the system by using cryptography, stenography and watermarking. In this work a system is proposed by applying visual cryptography technique to biometric template (retina). Visual cryptography technique has been applied on to the retinal template to make it secure from attack in centralized database as well as extra layer of authentication to the users.

1.1 Modules in Biometric System

There are basically two phases in biometric system. There are enrollment phase and authentication phase. In these two phases there are four modules. The sensor module is used in extracting the biometric data which may be image, audio or video. The feature extraction module is used in obtaining the template that is generated from the features of the biometric data. Each feature is labeled with a user's identity. The Matching module is used in authentication phase, where the template data is compared with data which is obtained from user and that it estimates the similarity between these data. These similar elements are processed in Decision making module which is used to identify the individual.

This work is organized as follow: Related work for security enhancement of biometrics system and various visual cryptography schemes are discussed in section2, section 3 presents the proposed system, experiments and results are shown in section 4, and section 5 concludes the work.

Manuscript received September 5, 2016
Manuscript revised September 20, 2016

2. Literature Survey

Ross and Asem (2011) explores the possibility of using visual cryptography for imparting privacy to biometric data such as fingerprint images, iris codes, and face images. In the case of faces, a private face image is dithered into two host face images (known as sheets) that are stored in two separate database servers such that the private image can be revealed only when both sheets are simultaneously available; at the same time, the individual sheet images do not reveal the identity of the private image. The purpose of Rajanwar et al (2014) is to protect biometrics data from the various attacks. We are using the concept of visual cryptography, where cryptography is the concept of sending and receiving encrypted messages and that can be decrypted by the authorized persons with the required keys only. Labati et al (2012) focuses on the most important privacy issues related to the use of biometrics, it presents actual guidelines for the implementation of privacy-protective biometric systems, and proposes a discussion of the methods for the protection of biometric data. A comprehensive survey of biometric cryptosystems and cancelable biometrics is presented by Rathgeb and Andreas (2011). State-of-the-art approaches are reviewed based on which an in-depth discussion and an outlook to future prospects are given. In this correspondence, Simoens et al (2012) analyze the vulnerabilities of biometric authentication protocols with respect to user and data privacy. The goal of an adversary in such context is not to bypass the authentication but to learn information either on biometric data or on users that are in the system. The design of single-use biometric security systems is analyzed by Lai et al (2011) from an information theoretic perspective. A fundamental trade-off between privacy, measured by the normalized equivocation rate of the biometric measurements, and security, measured by the rate of the key generated from the biometric measurements, is identified.

Hao et al (2013) propose a method using color histogram as the trait of retina biometric. The color histogram has shown the feature of deformation invariant. The enhancement using discrete wavelet transform decomposition minimizes the difference within the individuals and increases the correlation between the retinal images of the same person. Lajevardi et al (2013) presents an automatic retina verification framework based on the biometric graph matching (BGM) algorithm. The retinal vasculature is extracted using a family of matched filters in the frequency domain and morphological operators. Then, retinal templates are defined as formal spatial graphs derived from the retinal vasculature. Several multimodal biometric schemes have been suggested in literature which employs robust watermarking in order to embed biometric template data into biometric sample data. In case robust embedding is used as the sole means of security, tampering attacks can be mounted. The results of a corresponding attack against a multimodal iris recognition scheme show, that in this environment either semi-fragile watermarking or additional classical cryptographic means need to be applied to secure the system against the demonstrated attack which is presented by Hammerle et al (2011) Bringer et al (2011) introduces a new method to identify someone using his biometrics in an encrypted way. Our construction combines Bloom Filters with Storage and Locality-Sensitive Hashing. We apply this error-tolerant scheme, in a Hamming space, to achieve biometric identification in an efficient way. Arkala et al (2011) represent the retina vessel pattern as a spatial relational graph, and match features using error-correcting graph matching. They study the distinctiveness of the nodes (branching and crossing points) compared with that of the edges and other substructures (nodes of degree k, paths of length k).

Monwar et al (2011) utilize the physiological attributes (face, ear and iris) along with soft biometric information (gender, ethnicity and eye color). A fuzzy fusion mechanism for robust and reliable multimodal biometric based security systems is developed. Barkhoda et al (2011) proposed a novel human identification method based on retinal images. The proposed system composed of two main parts, feature extraction component and decision-making component. Instead of optimally aligning two iris-codes by maximizing the comparison score for several bit shifts utilizes the total series of comparison scores, avoiding any information loss. Blanton and Paolo (2011) develop and implement the first privacy-preserving identification protocol for iris codes. We also design and implement a secure protocol for fingerprint identification based on FingerCodes with a substantial improvement in the performance compared to existing solutions. Qamber et al (2012) present a system for recognition based on vascular pattern of human retina. The proposed algorithm consists of three stages; i.e. preprocessing, feature extraction and finally the matching process.

3. Research Methodology

This section gives the brief explanation of visual cryptography and methodology used for retina biometric privacy.

3.1 Visual Cryptography

Cryptography is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Naor and Shamir introduced the visual cryptography scheme (VCS) as a simple and secure way

to allow the secret sharing of images without any cryptographic computations. This scheme is referred to as the k-out-of-n VCS which is denoted as (k,n)VCS. Given an original binary image, it is encrypted in n images, such that

$$T = S_{h1} \oplus S_{h2} \oplus S_{h3} \oplus \dots\dots\dots\dots\dots S_{hn} \quad (1)$$

Where Å is a Boolean operation, Shi, hi *Î* 1, 2,….k is an image which appears as white noise, k d" n, and n is the number of noisy images. It is difficult to decipher the secret image T using individuals Shi's. The encryption is undertaken in such a way that k or more out of the n generated images are necessary for reconstructing the original image T. In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. For biometric privacy, here 2-out-of-2 scheme is using.

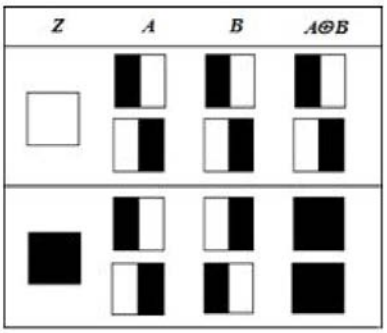

Fig I. Encoding A Binary Pixel P Into 2 Shares A And B

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 1 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.

3.2 Proposed Approach

As protecting template in the database securely is one of the challenges in any biometric system. Here visual cryptography technique is applied to retina authentication system. In this system there are two modules: Enrollment module and Authentication module. For accessing any secure resource by authenticated users this system can be used.

A. Enrollment

The administrator will collect the eye image of the eligible users those are having access to secure resource. The enrolled eye image is required to be processed so characteristic retinal features can be extracted. Three steps that are: segmentation, normalization, and feature extraction are performed as conferred below:

- Segmentation is performed to extract the retinal image from the eye.
- Normalization of retina region is carried out using sheet model. This model remaps each pixel within the retina region to a pair of polar coordinates.
- Feature extraction is done by convolving the normalized retina pattern into one dimensional wavelet.

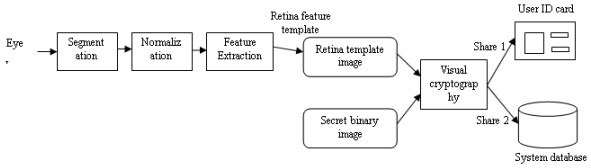

Fig. 2 User Enrollment

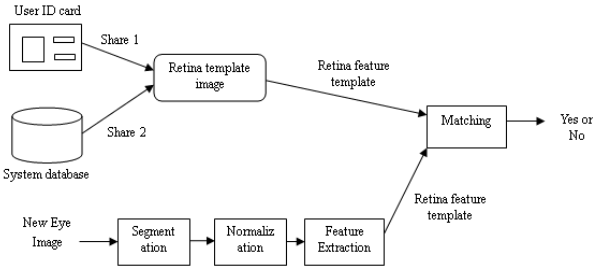

Fig. 3 User Authentication

In the existing system generated template is stored in the database. As Nalini K. Ratha et al pointed out that the stored template in the database attacker may try to alter result in authorization for unauthorized users, or denial of service for the authenticated user related with the corrupted template. Here retina template is protected by applying visual cryptography. For securing retina feature template, the template and another secret binary image which is chosen by system administrator is given as input to the visual cryptography. Two random shares are created with the help visual cryptography scheme. For sharing two secret images R1 is retina template image (generated from feature template) and R2 is secret image, two shares S1 and S2 are generated.

One share is stored in the database along with user login and other given to user on ID card along with login. Enrollment process is shown in the figure 2. As the visual

cryptography techniques guarantee that no information is revealed by one share alone, this provides security to the retina template in the database.

B. Authentication

For authentication user will provide share in the form of ID card. System finds the corresponding share from database. By stacking two shares first R1 retina template image is created. And from this image retina feature template is generated. The new eye image supplied by user will be processed with three steps: segmentation, normalization and feature extraction which generates retina feature template. Then these two feature templates are matched. If features match access is granted else the verification fails. Authentication process is shown in figure 3.

4. Experimental Results

The main intent of this work is providing security to the retina template in the database. To build this system, MATLAB platform is selected because of powerful inbuilt mathematical, signal and image processing functions of visual cryptography. Retina images are taken from DRIVE standard database.

Since the proposed technique was devised for binary eye images, a threshold value was used to generate the binary image for each probe. Each binary image was then decomposed into two sheets using VCS. The sheets were superimposed to get the target image. The reconstructed as well as the original grayscale retina probes were matched against the images in the gallery. These experiments suggest the possibility of decomposing and storing retina images. Two shares are generated Share1 and Share2 as output of visual cryptography algorithm. One share along with username is kept by system and other is given on the user ID Card. Table 2 shows the result of using the reconstructed retina as probes; the performance is reported as a function of the different threshold values used to binarize the original probe images. It is observed that a threshold of 180 results in an EER of 7.05%.

Table 1. Equal Error Rate (%) at different threshold values

Threshold	Equal Error Rate
120	28.2
150	14.6
180	7.05

For authentication user provides share which is on the ID card. The share extracted from this card is superimposed with corresponding share that is stored in the database, generates the retina template image as shown in figure 5. From this retina template image feature template is generated. Now this feature template is matched with retina feature of newly provided retina image.

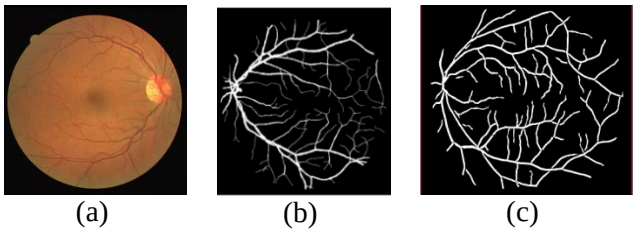

Fig. 4 (a) Retina Image (b) Retina segmentation (c) Extracted feature template

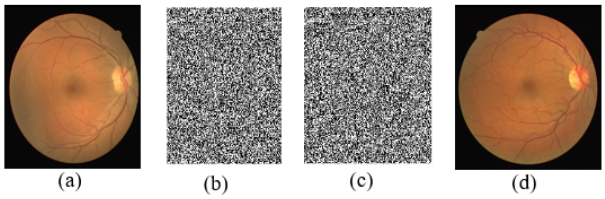

Fig. 5 (a) Retina template image (b) Share1 (c) Share2 (d) Result of superimposing of share1 and share 2

In this experiment, the possibility of exposing the identity of the secret image by using the sheet images in the matching process is investigated. For this experiment, the sheet images for three different Retina samples of the same subject were first computed. Next, the reconstructed images and the corresponding sheets were independently used in the matching process (i.e., sheet image 1 of all the private images were matched against each other; sheet image 2 of all the private images were matched against each other; reconstructed images of all the private images were matched against each other).The public datasets used in this experiments were datasets A. This experiment resulted in three EERs: the first was a result of using the reconstructed target images for matching, while the second and the third EERs were a result of using the first sheet and second sheet, respectively, for matching. The results in Table 3 confirm the difficulty of exposing the identity of the secret retina image by using the sheets alone.

Table 2.Equal Error Rate (%) for the experiment shows the individual shift images to reveal the secret images

	ERR (%)
Reconstructed vs Reconstructed	2.5
Sheet 1 vs Sheet 1	38.7
Sheet 2 vs Sheet 2	35.4

5. Conclusion

Various approaches adopted by researchers to secure the raw biometric data and template in database are discussed here. This work introduces the possibility of using visual cryptography scheme to provide the privacy to biometric data. A method is proposed to store retina template securely in the database using visual cryptography. In addition the contribution is here is also providing the privacy to the retina images private image can only be created only when both the sheets are present. Experimental results indicate that by applying visual cryptography techniques on retina template for more security, matching performance of iris recognition is unaffected with extra layer of authentication.

REFERENCES

[1] Ross, Arun, and Asem Othman. "Visual cryptography for biometric privacy."IEEE transactions on information forensics and security 6, no. 1 (2011): 70-81.

[2] Rajanwar, Shubhangi, Shirish Kumbar, and Akshay Jadhav. "Visual Cryptography for Biometric Privacy."

[3] Labati, Ruggero Donida, Vincenzo Piuri, and Fabio Scotti. "Biometric privacy protection: Guidelines and technologies." In E-Business and Telecommunications, pp. 3-19. Springer Berlin Heidelberg, 2012.

[4] Rathgeb, Christian, and Andreas Uhl. "A survey on biometric cryptosystems and cancelable biometrics." EURASIP Journal on Information Security 2011, no. 1 (2011): 1-25.

[5] Simoens, Koen, Julien Bringer, Hervé Chabanne, and Stefaan Seys. "A framework for analyzing template security and privacy in biometric authentication systems." Information Forensics and Security, IEEE Transactions on 7, no. 2 (2012): 833-841.

[6] Lai, Lifeng, Siu-Wai Ho, and H. Vincent Poor. "Privacy–Security Trade-Offs in Biometric Security Systems—Part I: Single Use Case." Information Forensics and Security, IEEE Transactions on 6, no. 1 (2011): 122-139.

[7] Hao, Hao, Dinesh Kant Kumar, Behzad Aliahmad, M. Z. Che Azemin, and R. Kawasaki. "Using color histogram as the trait of retina biometric." In Biosignals and Biorobotics Conference (BRC), 2013 ISSNIP, pp. 1-4. IEEE, 2013.

[8] Lajevardi, Seyed Mehdi, Arathi Arakala, Stephen A. Davis, and Kathy J. Horadam. "Retina verification system based on biometric graph matching."Image Processing, IEEE Transactions on 22, no. 9 (2013): 3625-3635.

[9] Hämmerle-Uhl, Jutta, Karl Raab, and Andreas Uhl. "Attack against robust watermarking-based multimodal biometric recognition systems." In Biometrics and ID Management, pp. 25-36. Springer Berlin Heidelberg, 2011.

[10] Bringer, Julien, Hervé Chabanne, and Bruno Kindarji. "Identification with encrypted biometric data." Security and Communication Networks 4, no. 5 (2011): 548-562.

[11] Arakala, Arathi, Stephen A. Davis, and Kathy J. Horadam. "Retina features based on vessel graph substructures." In Biometrics (IJCB), 2011 International Joint Conference on, pp. 1-6. IEEE, 2011.

[12] Monwar, Md Maruf, Marina Gavrilova, and Yingxu Wang. "A novel fuzzy multimodal information fusion technology for human biometric traits identification." In Cognitive Informatics & Cognitive Computing (ICCI* CC), 2011 10th IEEE International Conference on, pp. 112-119. IEEE, 2011.

[13] Barkhoda, Wafa, Fardin Akhlaqian, Mehran Deljavan Amiri, and Mohammad Sadeq Nouroozzadeh. "Retina identification based on the pattern of blood vessels using fuzzy logic." EURASIP Journal on Advances in Signal Processing 2011, no. 1 (2011): 1-8.

[14] Blanton, Marina, and Paolo Gasti. "Secure and efficient protocols for iris and fingerprint identification." In Computer Security–ESORICS 2011, pp. 190-209. Springer Berlin Heidelberg, 2011.

[15] Qamber, Sana, Zahar Waheed, and M. Usman Akram. "Personal identification system based on vascular pattern of human retina." In Biomedical Engineering Conference (CIBEC), 2012 Cairo International, pp. 64-67. IEEE, 2012.