I J C T A, 9(40) 2016, pp. 247-255
© International Science Press

Protection of Fused Template Using Visual Cryptography

Sukhdev Singh[*] and Chander Kant[**]

ABSTRACT

Template protection is a challenging task in the field of biometric systems. Multimodal biometrics is an emergent technology in this field because of its high security features. In this paper, a novel approach is proposed to secure fused template of Iris and Finger Knuckle Print (FKP) by using visual cryptography. Visual cryptography is a secret sharing scheme where a fused template is encrypted into the number of shares, which independently disclose no information about the original fused template. The experimental work in the proposed work shows the efficiency of visual cryptography for securing fused template.

Keywords: Biometrics, Finger Knuckle print, IRIS and Visual Cryptography

I. INTRODUCTION

Biometrics technology is related to physiological or behavioural characteristics of a person to authenticate identity of the person for security purposes. Biometric authentication is getting more concentration for automated personal identification than other methods of authentication like password and ID cards. There are various applications where personal identification is required such as computer login control, passport control, secure electronic banking, mobile phones, bank ATM, credit cards, border crossing, airport premises access control, health and social services and Aadhaar card in India. There are many biometric techniques for authentication based on physical or behavioural characteristics of the person such as facial thermogram, ear, hand geometry, fingerprint, finger knuckle print, face, retina, iris, palm print, hand vein, gait, keystroke, odor, voice and signature. Among these traits, iris and finger knuckle print are the most promising biometric because of their stability, uniqueness and non-invasiveness [1]. Biometric system with single trait of person is called the unimodal biometric system and it cannot give us perfect identification and result. To overcome this disadvantage of unimodal systems, a multimodal biometric system is used.

In multimodal biometrics systems more than one trait are used and there are certain vulnerability related to these biometric template. Biometrics templates are uniquely inherent and cannot be re-issued or replaced in the case of stolen. Different biometric template protection schemes are shown in fig.1. Hence various researches have been proposed to protect the templates by using cryptography, steganography and watermarking. Jain et al. [2] depicted four principles for biometric template protection scheme. Firstly it should be revocable and put a new template in database based on the same biometric trait. Secondly if a revoked template is replaced by anyone with fraud, it should not be like as previous one. Its computational properties ensure the user's privacy. Thirdly it should be difficult to obtain the original template from the protected template with any computational task. Finally the implemented protection approach improves the recognition performance of system beside the degradation. Thus protection mechanism of biometrics templates is very essential in any biometric system whether it is unimodal or multimodal biometric systems.

[*] Research Scholar, Department of Computer Science & Applications, Kurukshetra University, Kurukshetra, Haryana, India, *E-mail: sukhdev_kuk@rediffmail.com*

[**] Department of Computer Science & Applications, Kurukshetra University, Kurukshetra, Haryana, India, *E-mail: ckverma@rediffmail.com*

This paper proposed an approach to protect the fused template of iris and finger knuckle print by using visual cryptography scheme. It is used for secret communication and storage of biometrics templates in a dispersed format. Naor and et al. [3] introduced visual cryptographic scheme, it is a simple secret sharing scheme used to encrypt the visual information and the decryption is done by human visual system. There are various visual cryptography schemes (VCS) e.g. k-out-of-n , for general access structure, recursive threshold, Halftone, for grey images, for colour images, multiple secret sharing scheme, extended, progressive, region incrementing and segment based VCS. This paper refers to the k-out-of-n VCS which is denoted by VCS (2, 2). Here VCS shares of images will be generated based on the pixel as shown in table 1.

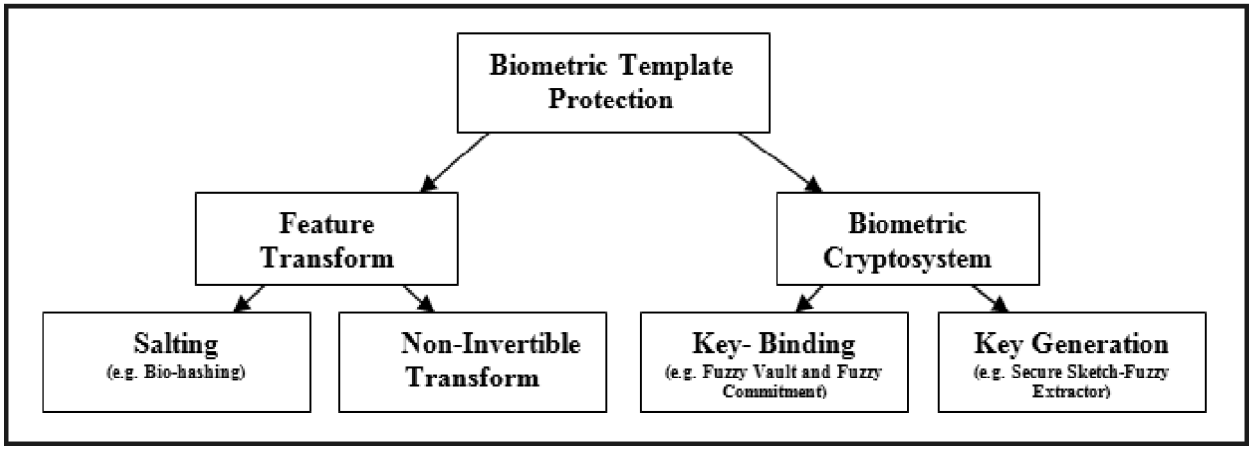

Figure 1: Existing template protection schemes

This paper is organized as follows: section II presents the related works for template protection of biometric systems using visual cryptography scheme, section III presents the proposed approach, section IV shows the results and discussion, and finally concluding observations are given in section V.

Table 1
Encoding binary image into two shares [3]

Pixel	Probability	Shares #1	Shares #2	Superposition of the two shares	
	$p = 0.5$				White Pixels
	$p = 0.5$				
	$p = 0.5$				Black Pixels
	$p = 0.5$				

II. RELATED WORKS

To improve the privacy and security of multimodal biometrics templates, visual cryptographic scheme is used with biometric fused template. Some related works with this scheme have been studied which are listed below.

Thomas Monoth et al. [4] proposed visual cryptographic scheme for the finger print image for provide secure transmission. The fingerprint image is broken into a number of shares which does not reveal any visible and computational information about the finger image. These shares are distributed to a number of

participants. The original fingerprint is generated only by stacking number of shares which is necessary. The reconstruction of the secret image is based on XNOR operation.

Arun Ross et al. [5] proposed multiple biometric system for preserving the digital biometric data (face image) using visual cryptography scheme. In their proposed work they have used multiple faces to improve the security level in biometrics. Secret image is dithered into two other images; these shares are stored in two different database. The secret face image is appeared only when both the shares are available at the same time. To recover original template XOR operator is used. It is difficult to identify the secrets with one share.

Vionthini et al. [6] introduced biometric based visual cryptography scheme to solve the authentication issues. Stenographed fingerprint image is used, which is separated into two shares, one is stored in the bank database and other one is given to the customer. Hash code is generator for each customer shares and this code is stored in the bank database. During the transaction the customer provides the shares. The shares are verified for the transaction with the other share that is stored in the database for the access. This improves the security level in biometrics.

Ankita Gharat et al. [7] used visual cryptography with pixel sharing for the biometric data such as fingerprint image. To protect the biometric data from unavoidable hacking from the attackers, visual cryptographic scheme is applied in biometric data. Two shares are generated from the biometric image that are stored in two separate database after the encryption is applies. To recover the biometric image XOR operator is used.

Shital B. patil et al. [8] introduced biometric privacy to protect important data from attacks. By using visual cryptographic technique, face image is separated into two host images and these shares are saved in two different database. The original image is retrieved only by stacking both the shares .The single share which does not provide any information about the original biometric data.

Harkeerat Kaur et al. [9] introduced biometric template protection using cancellable biometrics and visual cryptography techniques. They proposed the biometric template protection mechanism by using cancellable biometrics and visual cryptographic technique.

N. Radha et al. [10] in their proposed work they have applied visual cryptography technique to secure the template authentication of finger vein and signature in multimodal biometric. In proposed work the fusion technique is used to fuse finger vein and signature images after that they have applied visual cryptography scheme for generate the share of the biometric template. They have evaluated the proposed work with evaluation metrics FAR, FRR and accuracy.

III. PROPOSED WORK

In multimodal biometric systems, attacks against the database are a big challenge. To solve this problem related with template security, an approach is presented for securing iris and finger knuckle print fused template in database with visual cryptography. It is used to protect the template in database from attackers and hackers. If an attacker or hacker somehow succeeds in tampering to database templates, he can tamper or damage only incomplete templates from the database. It would be completely impossible for him to access the original fused template of iris and finger knuckle print due to proposed approach.

3.1. Iris Preprocessing and Feature Extraction

Among all biometric traits iris is considered most accurate traits for recognition because it has low false acceptance ratio (FAR) and false rejection rate (FRR) with high accuracy. In proposed approach iris preprocessing stage consists of three steps, (i) Segmentation (ii) Normalization (iii) Feature extraction. These steps are described below. Basic steps for iris feature extraction are shown in fig. 2.

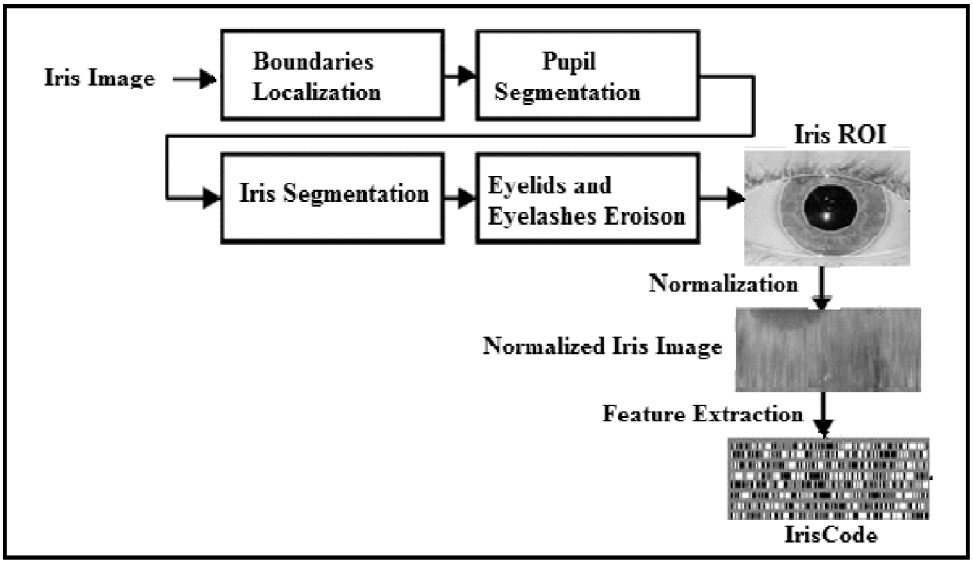

Figure 2: Steps for iris feature set extraction

(i) Iris Segmentation: In this process a sensor captures an iris image with desirable resolution and contrast. In capturing process sensor captures the larger image containing data from surrounding area of eye also. Before performing the iris segmentation it is necessary to localize the area corresponding to iris and segmentation of pupil. It provides the accurate position of circular iris. Iris region is bounded by two circles which are sensed by Circular Hough transform [11] for segmentation. To select the ROI of iris eyelid removal using canny edge detection and eyelashes are removed by threshold value.

(ii) Iris Normalization: Size of iris has different patterns from person to person and individual to individual due to illumination variability, size of the pupil and distance of eye from the capturing camera. These issues can change matching results in feature set. To get accurate iris matching results, it is necessary to reduce these problems. To sort out these problems, the localized iris is converted into polar-coordinates by remapping each point within the iris region with the help of Daugman's Rubber Sheet Model [12].

(iii) Feature Extraction: Feature extraction is the process of converting original image into binary image. After locating the iris image, it is encoded to an Iris Code that is the 2048-bit representation of iris pattern. 2D Gabor filter is used for extracting the features from the normalized iris image [13, 14].

3.2. FKP Preprocessing and Feature Extraction

There are three bones in our each finger, i.e. (i) proximal phalanx, (ii) middle and (iii) distal phalanx. The first joint is called the proximal phalanx. The second joint is the proximal interphalangeal joint and third joint is called distal phalanx. Finger knuckles of the human hand are characterized by the creases on back surface of a finger on the human hand. These creases differ from person to person. The usages of finger knuckle print for personal authentication gives the promising result and attract the researchers for this trait of biometric. The FKP preprocessing and feature extraction have following steps that are shown in fig. 3[15]:

(i) Capture the FKP images through data acquisition device.

(ii) Localization of Region of Interest for the feature extraction.

(iii) Extracting segmented FKP image: ROI is to be automatically extracted using edge detection approach. This gives the segmented finger knuckle image.

(iv) FKP image enhancement by using image enhancement techniques.

(v) Linear Discriminant Analysis technique is used to extract the features from FKP images, it extracts significant features from FKP image with low dimensionality of the feature set [16] [17].

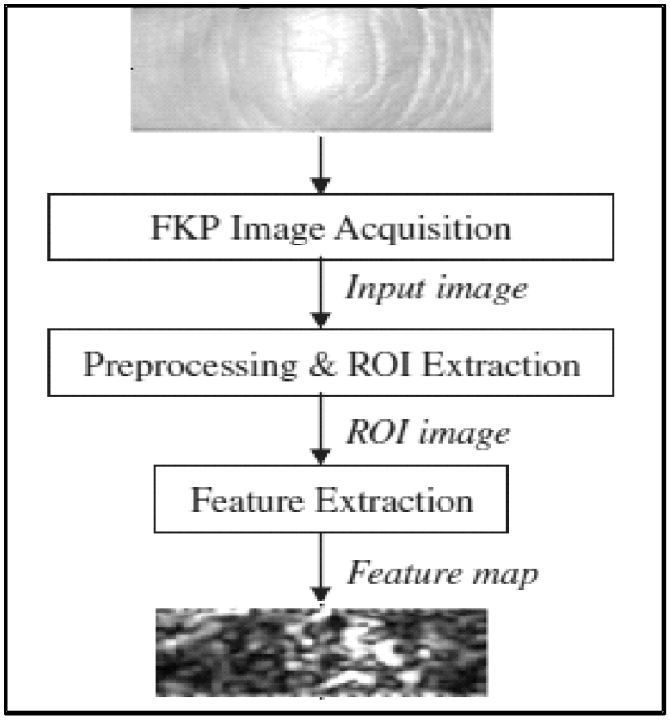

Figure 3: Steps for finger knuckle print feature set extraction

3.3. Architecture of Proposed Approach

Figure 4 shows the block diagram of the proposed approach to protect the template by using visual cryptography. The proposed approach is using two biometric traits iris and finger knuckle print. It has some phases which include: image preprocessing, feature extraction, fusion at feature level, share generation using visual cryptography, matching and decision making. In the proposed enrollment approach, different biometric sensors capture the two biometric traits individually from the person and convert them into feature set. Fused template is generated by combining the individual feature set with feature level fusion. Finally the fused template is converted into two shares by using visual cryptography scheme. One share is stored in server database and other is stored in user id. In the proposed verification approach, again different biometric sensors capture the two biometric traits individually from the person and convert them into feature set. Fused feature set of both traits will be compared with template and it will be recovered from share1 and share2 by the visual cryptography.

(i) Fusion at Feature Level: The feature sets of iris and finger knuckle print are combined at feature level to generate a fused feature set. As feature set from individual traits are heterogeneous, due to difference in extraction method. It leads very high variability. In order to remove this variability normalization method z-score is used [18]. It is calculated by using the arithmetic mean and standard deviation of the different feature sets.

$$x'_k = \frac{x_k - \mu}{\sigma} \tag{1}$$

After normalization, the feature sets of X_{iris} and X_{fkp} are combined with normalized X'_{iris} and X'_{fkp} feature sets. And it will produce the fused template for enrollment and verification process for proposed approach.

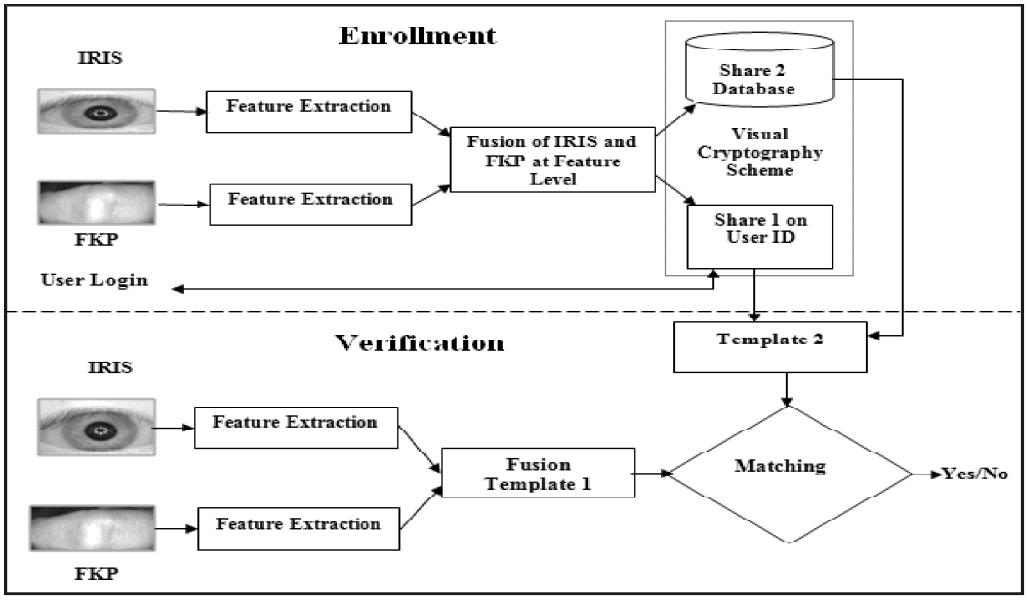

Figure 4: A block-diagram of proposed approach for template protection using visual cryptography

(ii) Working Principle of Visual Cryptography: In visual cryptography scheme every pixel of the template is converted into four sub pixels of two share images and is recovered by using the logical OR operation between the shares. The four sub pixels are generated from a pixel of the template in a way that two sub pixels are white and two sub pixels are black. The black or white pixel selection is based on random selection. As shown in fig.5 share generation and stacking of template have the following steps [3]:

Step 1: Take template of multibiometric system.

Step 2: Use the method visual cryptography to expand each pixel into 2 X 2 blocks arrays of template.

Step 3: Two transparent shares of template have generated and stored in respective database.

Step 4: Stacking of share of two transparent shares will produce the template for verification process.

Step 5: Finally matching process for genuine or imposter templates will be done by using hamming distance algorithm.

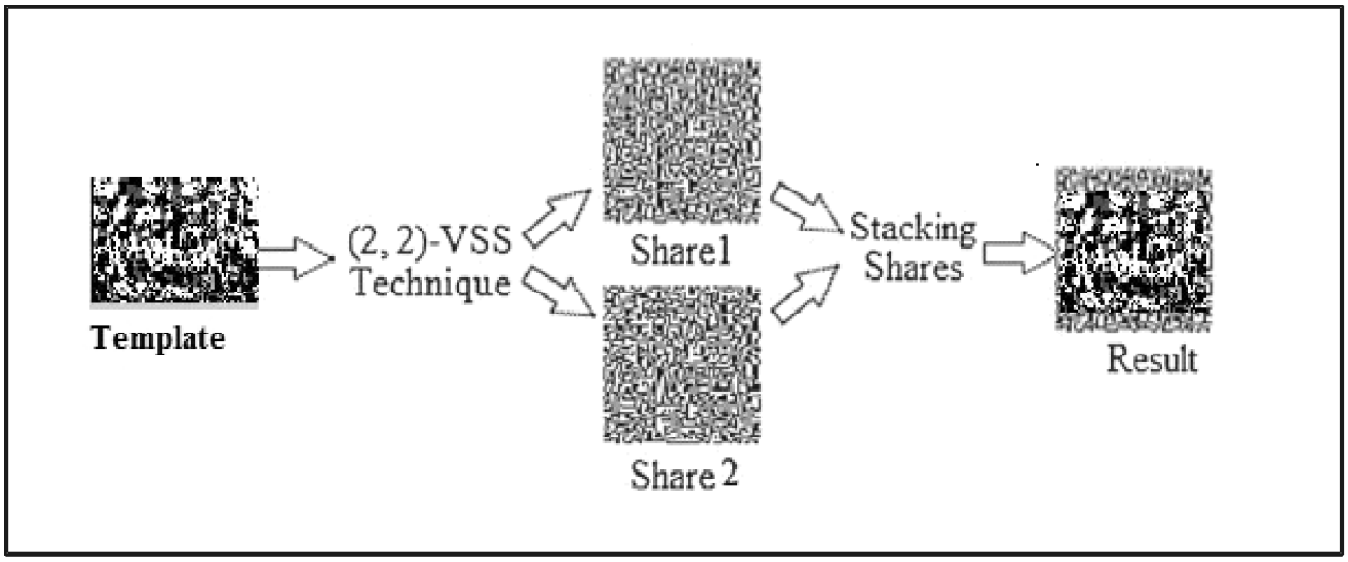

Figure 5: Block diagram of visual cryptography

IV. RESULT AND DISCUSSION

4.1. Databases

Two different databases (Iris and FKP) are used in the proposed approach. For iris we have used CASIA-Iris V1 database [19] contains 756 images from 108 eyes. All images are stored as bitmap picture format with resolution 320 X 280 is shown in Fig.6. For Finger Knuckle Print, we have used FKP images of PolyU database and it contains the 7,920 images from 660 different fingers of 165 volunteers is shown in fig.7 [20].

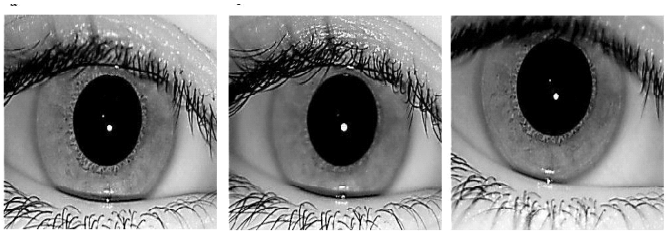

Figure 6: Sample images from CASIA Iris database

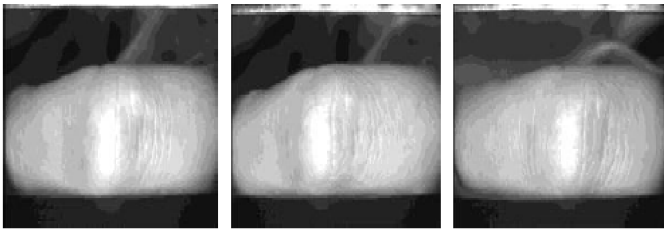

Figure 7: Sample images of Finger Knuckle Print

4.2. Performance Measurement

This paper shows enrollment and verification process of multimodal biometric with template protection by using visual cryptography. The proposed approach fulfills four biometric template protection criteria as discussed in the section I. These four criteria specified by Jain et al. [2] for template protection. These are following:

(i) Diversity: Fused template of biometric systems has decomposed into different constituting shares, by using visual cryptography scheme. Fused template is divided into different share, so it is impossible to collect the share for an attacker.

(ii) Revocability: Visual cryptography scheme is used some predefined or randomly selected supporting data while generating shares. These shares can be replaced any time to produce revocable template. So revocability of a template is possible in the case of attacks.

(iii) Security: It is more difficult to obtain the fused template image by any individual share less than required number. In this case security is improved and anyone cannot breach the security of fused template.

(iv) Performance: The performance of proposed approach does not degrade when the original fused template is reconstructed from its constituting shares by using visual cryptography scheme with proposed approach. FAR, FRR and GAR are determined as follow:

$$FA\ R\ (\%) = \frac{wrongly\ accepted\ individuals}{total\ number\ of\ wrong\ match} \times 100\% \tag{2}$$

$$FRR\ (\%) = \frac{wrongly\ rejected\ individuals}{total\ number\ of\ correct\ matching} \times 100\% \tag{3}$$

$$GAR\ (\%) = (100\text{-}FRR\ \%) \tag{4}$$

$$Accuracy\ (\%) = (100\text{-}(FAR\%+FRR\ \%)\ /2) \tag{5}$$

Table 2
Best FAR and FRR ratio for proposed approach

Threshold	*FAR (%)*	*FRR (%)*
0.72	0.00	82
0.77	0.07	77.25
0.79	0.08	43.33
0.82	0.40	32
0.85	2.5	2.8
0.89	22	9.99
0.91	30	8
0.96	59	3
1.00	91	2

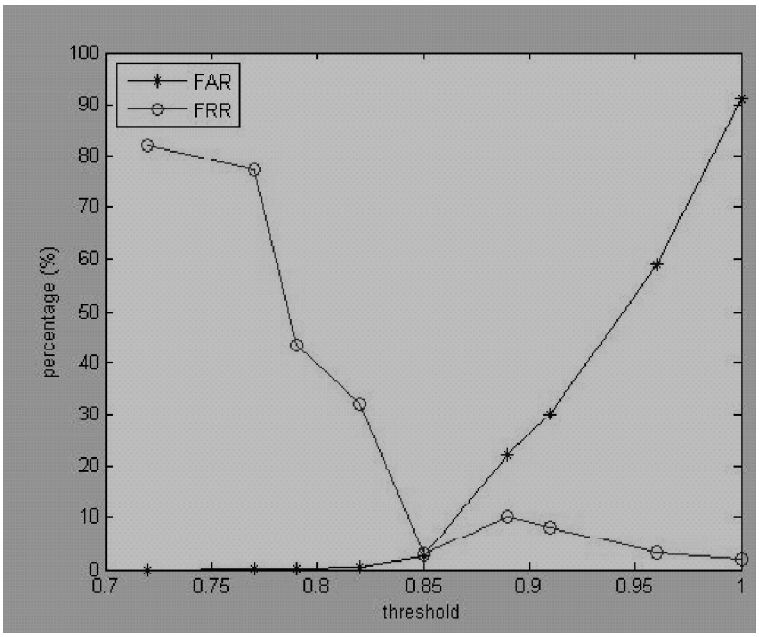

Figure 8: ROC Curve for EER (0.85%) in proposed approach

Visual cryptographic scheme has applied on the fused template to protect the original biometric template and it doesn't decrease performance of the biometric system. System performance is calculated in Matlab 2014a with minimum FAR of 2.5%, FRR of 2.8% and accuracy of 97.5% has shown in table 2. Equal Error Rate (EER) on best FAR and FRR are shown in fig. 8.

V. CONCLUSION

This paper explores an approach to protect the fused template of iris and finger knuckle print using visual cryptography in a multimodal biometric system. Since the spatial arrangement of the pixels in these images varies from block to block, it is impossible to recover the original template without accessing both the shares. In addition to this, the proposed work has also improved the accuracy of the protected fused template by superimposing the two noisy images, and is finally fully recovered the original template without any noise. The biometric images are pre-processed and features are extracted from iris and finger knuckle print images by using 2D Gabor filter and Linear Discriminant Analysis (LDA) simultaneously. The experimental results also authenticate the security and accuracy of the proposed approach. In future, the proposed approach

can be done by applying other visual cryptographic schemes (multiple secret sharing, extended, progressive, Halftone etc.) that may improve the authentication level in other sophisticated area.

REFERENCES

[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] Jain AK, Nandakumar K, Nagar A, et al. (2008) Biometric template security. EURASIP Journal on Advances in Signal Processing 2008.

[3] Naor, Shamir, "Visual cryptography" Advances in cryptology- Eurocrypt'94, pp. 1-12.

[4] Thomas Monoth, Babu Anto, "Tamper proof transmission of fingerprints using visual cryptography schemes", ELSEVEIR, 2010, Vol. 2, No. 3, pp. 143-148.

[5] Arun Ross, Asem Othman, "Visual cryptography for biometric privacy", IEEE Transactions on Information Forensics and Security, 2011, Vol. 6, No. 1, pp. 70-80.

[6] Vinodhini, Premanand, Natrajan, "Visual cryptography using two factor biometric system for trust worthy authendication", International journal of scientific and research publications, 2012, Vol. 3, No. 3, pp. 1-5.

[7] Ankita Gharat, Preeti Tambre, "Biometric privacy using visual cryptography", International journal of advanced research in computer engineering and technology, 2013, Vol. 2, No. 1, pp. 180-185.

[8] Shitlal Patil, Um Nagaraj, "Preservation of biometric data using visual cryptography", International journal of computer technology and applications, 2014, Vol. 5, No. 3, pp. 937-940.

[9] Harkeerat Kaur, and Pritee Khanna. "Biometric template protection using cancelable biometrics and visual cryptography techniques." Multimedia Tools and Applications (2015): 1-29.

[10] Nandhinipreetha, A., and N. Radha. "Multimodal biometric template authentication of finger vein and signature using visual cryptography." 2016 International Conference on Computer Communication and Informatics (ICCCI). IEEE, 2016.

[11] R. Wildes, J. Asmuth, G. Green, S. Hsu, and S. Mcbride. "A System for Automated Iris Recognition", Proceedings IEEE Workshop on Applications of Computer Vision, Sarasota, FL, USA, 1994.

[12] J. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence," IEEE Trans. Pattern Anal. Machine Intell, vol. 15, pp. 1148-61, 1993.

[13] D.Gabor, " Theory of communication ", J. inst. Elect. Eng. London, Vol. 93, No. III, 1946.

[14] A. Kumar and A. Passi, "Comparison and Combination of Iris Matchers for Reliable Personal Aauthentication," Pattern Recogniion., Vol. 23, No. 3, pp. 1016–1026, March 2010.

[15] A. Kumar and C. Ravikanth, "Personal authentication using finger knuckle surface", IEEE Trans. Info. Forensics & Security, vol. 4, no. 1, pp. 98-110, March 2009.

[16] H. Yu and J. Yang, "A direct LDA algorithm for high dimensional data with application to face recognition," Pattern Recognition, September 2001.

[17] P. Navarrete and J. Ruiz-del-Solar, "Analysis and Comparison of Eigenspace-Based Face Recognition Approaches," International Journal of Pattern Recognition and Artificial Intelligence, Vol. 16, No. 7, November 2002.

[18] Rattani, Ajita, et al. "Feature level fusion of face and fingerprint biometrics." Biometrics: Theory, Applications, and Systems, 2007. BTAS 2007. First IEEE International Conference on. IEEE, 2007.

[19] Chinese Academy of Science - Institute of Automation, Database of the Eye Grayscale Images. *http:// www.sinobiometrics.com*

[20] PolyU Finger Knuckle Print Database., availableat: http://www.comp.polyu.edu.hk/~biometrics/FKP.htm, last visited 2014.