ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

A Novel Multiple Secret Sharing Scheme for Biometric Iris Template

M.Arunadevi[1], Dr. V. Palanisamy[2]

[1]Research Scholar, [2]Professor
Department of Computer Science and Engineering, Alagappa University,
Karaikudi-600 003, Tamilnadu, India.
[1]arunadevi.mab@gmail.com,[2]vpazhanisamy@yahoo.com

***Abstract*— Biometrics deals with verify/recognize a person depend upon his physical/behavioral characteristics. VC is a term of Visual Cryptography in which image is decomposed into different shares. Therefore, when all these shares are stacked together, original image is obtained and so there is no possibility to view the image with one share. If this multiple secret sharing scheme is combined with biometrics, provide efficient way to secure the biometric templates. Many researchers have proposed method based on the combination of visual cryptography and biometrics. This paper proposes a novel multi share creation procedure for protecting the iris template. In this method, Biometric iris image is converting in to grayscale image and from that image, pixels are taken, divide by number 4 and by use of result, create basic matrices. Then Key matrix is generated and after that, XOR operation is done on key matrix and basic matrices to create shares. If all of these shares are stacked together, iris template is recovered.**

***Keywords*— Biometrics, Iris template, Visual cryptography, Shares, XOR, .**

I. INTRODUCTION

Biometrics is used to identify individual person uniquely using their physical, chemical or behavioral traits [1].It is an efficient way to protect the data at the same time there is a chance to attacker can access the database. So the security and privacy of biometric system is a major concern due to some issue like fake biometrics, override matcher [2]. So, there is need to preserve the privacy of biometric data. In this paper, biometric data is protected use of VC (Visual Cryptography). Naor and Shamir's proposed the visual cryptography [3] which is allowed to secret sharing images without cryptographic computation and this scheme is refer as K-out-of-n VCS. Original image is given and get encrypted form of n images as follows:

$$T = S_{h1} \oplus S_{h2} \oplus S_{h3} \oplus .....S_{hn}$$

where $\oplus$ is a boolean operation, S_{hi}, $h_i \in 1, 2, ..., k$ is an image which appears as white noise, $k \leqslant n$, and n is the number of noisy images. It is difficult to decipher the secret image T using individual S_{hi}' s. [4] In Visual cryptography, a secret binary image is programmed into n shares of arbitrary binary prototypes. It is possible to decode the secret image visually by superimposing a qualified subset of transparencies. Nevertheless no secret data can be acquired from the superposition of an illegal subset [5]. Extended VC is proposed by [6] in which shares have secrets but these shares are meaningful shares. In EVC, each share is some meaningful image rather than random collection of black & white pixels. Visual cryptography is developed for black and white images only till 1997. Visual cryptography scheme used firstly for the color image by [7] but meaningless shares. Chang et al. [8] proposed visual cryptography for colored images with meaningful shares. Hou *et al.* [9] proposed VC scheme for gray level images which is based on halftone technique & color decomposition method. The security is enhanced when VCS is combined with Biometric. Original image is divided into shares and stored in individual database. Single share can't reveal the secret image. When all the shares are available, original image is retrieved with high level of secure. The rest of the paper is organized as follows: In section 2, related work is discussed. In section 3, proposed method is described and implemented. In section 4, experiment is done on iris sample image and result is produced. In section 5, conclusion is given.

II. RELATED WORK

Ankita Gharat *et al.* [10] have proposed method in which use the visual cryptography scheme for the biometric privacy. In this method, biometric templates are split into two images. Here, utilization of XOR operator, superimposing the two images and can recover original template. When all the shares are accessed and stacked, original template is obtained. Therefore, there constructed image will be visually appealing while requiring less storage space.

Arun Ross *et al.* [11] have proposed visual cryptography based method for face biometric image privacy. Here security level of biometric is enhanced by use of multiple faces. In this

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

method, Face image is dithering in two shares and these shares are stored in database separately. To get back the original image, XOR operator is used. Thus, it is not possible to find the secrets with single share and so reveal the secrets by stacking all the shares.

The method proposed by Rahna *et al.* [12] in which the templates are scrambled and decomposed into two noise-like images using (2,2) VCS, and since the spatial arrangement of the pixels in these images varies from block to block, it is impossible to recover the scrambled image without accessing both the shares and an XOR operator is used to superimpose the two noisy images to get the scrambled image.

Divya James *et al.* [13] have introduced a novel method for securing face templates by Chaos and visual cryptography techniques. In this novel method, face image is decomposed into two host images by using digital Halftoning, pixel expansion and encryption principle of gray-level extended VC scheme. Then 3d chaotic map encryption algorithm is applied on each shares. With this novel scheme, one can verify identity with both protection and privacy.

The method proposed by Biruntha.S *et al.* [14] which provide security for biometric data using non expansible VC scheme. In this method, read biometric data as an input and this image is decomposed into 2 shares. Then 2nd share is rotated into180 degree. These shares are overlapped and image is decrypted, matched when users are entered and matching with system generation of biometric image..

III. PROPOSED METHOD

The proposed method is used to secure the biometric iris image and this image is dividing into shares with the novel share creation scheme and when all shares are stacked together only, original iris image is obtained. In this method, read iris image from database and it is converting into grayscale image. Then pixel values are extracted from that image and after that, each and every pixel is divided by 4 and result values are placed into I_1, I_2, I_3, and I_4 which is called basic matrices. If remainder value is obtained, it is carry on based on number values.

The block diagram of proposed work is shown in Figure 1.

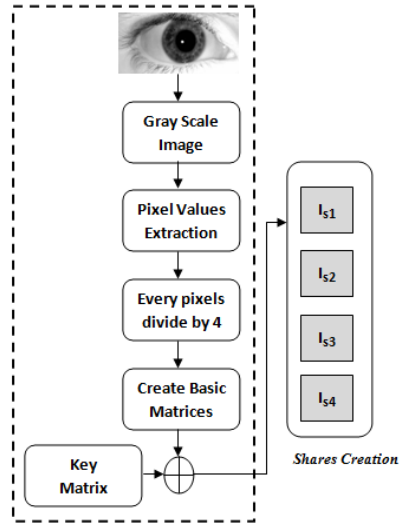


Fig.1 Block diagram of proposed method

For example, take pixel value 100 from image and it is divided by 4.So, corresponding pixel values of I_1 matrix is 25, I_2 matrix is 25, I_3 matrix is 25 and I_4 matrix is 25. Let consider another example, suppose pixel value 102 is taken from image and it is divided by 4, its remainder value is 2. Now corresponding pixel values of I_1 matrix is 25, I_2 matrix is 27, I_3 matrix is 25 and I_4 matrix is 25. After that, key matrix is generated randomly and values in key matrix are XORed with values in basic matrices to create 4 shares. Here, number of basic matrices is 4 and so number of shares is 4. When all the shares are combined together, get original iris image. Otherwise, it produces different images.

Following novel algorithm is used to secure iris image

Step 1: Read Iris image as an input from database

Step 2: Image is convert into grayscale format

Step 3: Extracting pixels, P_i , from that image.

Step 4: Based on the pixels extraction, create 4 basic matrices namely, I_1, I_2, I_3, and I_4.

Step 5: After that, every pixels are divided by 4 and its result values are stored in corresponding pixel values of basic matrices. Suppose if it has remainder value, it is placed in number values of basic matrices Example as shown in fig.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Sample Pixel Value	I_1	I_2	I_3	I_4
100	25	25	25	25
101	26	25	25	25
102	25	27	25	25
103	25	25	28	25

Sample Pixel Value	I_1	I_2	I_3	I_4
104	26	26	26	26
105	27	26	26	26
106	26	28	26	26
107	26	26	29	26

Sample Pixel Value	I_1	I_2	I_3	I_4
108	27	27	27	27
109	28	27	27	27
110	27	29	27	27
111	27	27	30	27

Sample Pixel Value	I_1	I_2	I_3	I_4
112	28	28	28	28
113	29	28	28	28
114	28	30	28	28
115	28	28	31	28

Step 6: Generating a key matrix, K_m , randomly based on the size of basic matrices.

Step 7: Then, Share creation process is performed using XOR operation and novel share creation procedure. To create four shares, elements in the key matrix is XORed with elements in basic matrices,

$$I_{s1} = (K_{m00} \oplus I_{11}) + (K_{m01} \oplus I_{12}) + (K_{m10} \oplus I_{13})\,(K_{m11} \oplus I_{14})$$

$$I_{s2} = (K_{m00} \oplus I_{21}) + (K_{m01} \oplus I_{22}) + (K_{m10} \oplus I_{23})\,(K_{m11} \oplus I_{24})$$

$$I_{s3} = (K_{m00} \oplus I_{31}) + (K_{m01} \oplus I_{32}) + (K_{m10} \oplus I_{33})\,(K_{m11} \oplus I_{34})$$

$$I_{s4} = (K_{m00} \oplus I_{41}) + (K_{m01} \oplus I_{42}) + (K_{m10} \oplus I_{43})\,(K_{m11} \oplus I_{44})$$

Step 8: Now shares are created. Thus, Iris image is divided into meaningful shares.

Step 9: When we want to get back original iris image, all shares are stacked together by performing XOR and subtraction operation.

IV. Result and Discussions

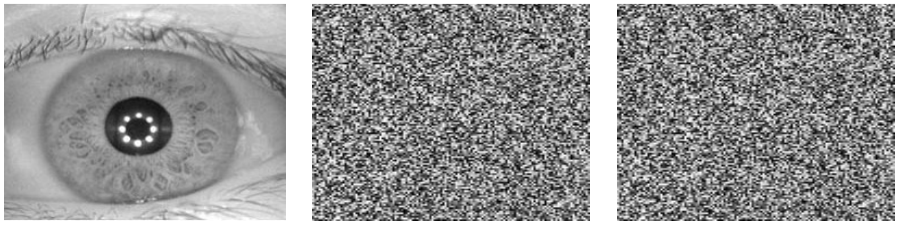
A. Experimental Results

In order to evaluate and check the performance of the proposed algorithm i.e. Bio-chaotic algorithm we took iris images from one of the renowned database CASIA (Chinese Academy of sciences and institute of Automation) [7]. The database contains a lot of iris images taken from different people eyes. In our case we use 3 of the iris images from this database to carry out our experimental process. These images are shown in fig.2, 3 and 4 respectively.

(a) Secret Iris image (b) Share 1 (c) Share 1

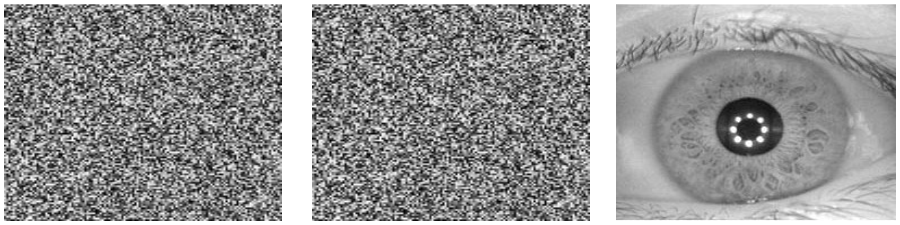
(d) Share 1 (e) Share 1 (f) Reconstructed Iris image

Figure 2. Sample Iris images in CASIA-Iris-Twins



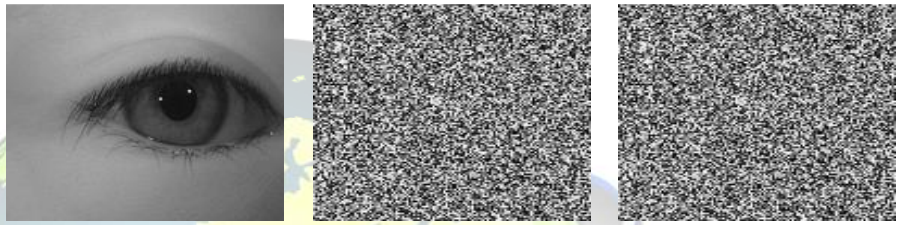
ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

(a) Secret Iris image (b) Share 1 (c) Share 1

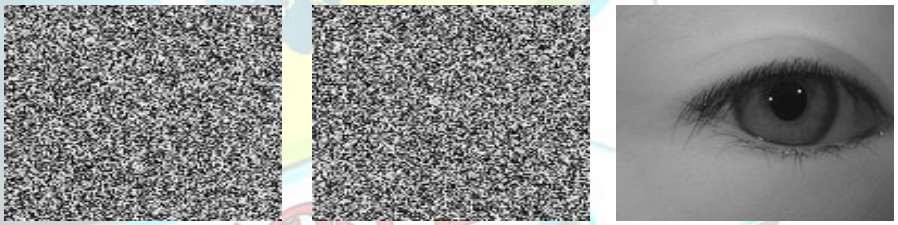


(d) Share 1 (e) Share 1 (f) Reconstructed Iris image

Figure 3. Iris images in CASIA-Iris-Interval



(a) Secret Iris image (b) Share 1 (c) Share 1



(d) Share 1 (e) Share 1 (f) Reconstructed Iris image

Figure 4. Sample Iris images in CASIA-Iris-Twins

V. CONCLUSION

In this paper we have presented a novel multiple secret sharing schemes for biometric Iris Template. It is very secure against server side attack on biometric template. Because this iris template is divided into multiple shares which only all shares are taken for authentication where original iris template. The proposed multiple secret sharing schemes recommended a more secured approach for iris biometric data privacy. The proposed multiple secret schemes achieved all the security requirements of VC and hence offer better security.

REFERENCES

[1] A. Jain, P. Flynn, and A. Ross, "Handbook of Biometrics", Springer, 2007

[2] Shubhangi Kahulkar, Samiksha Patil, Prajkta Bhoir, Jayesh Kulkarni, Prof. Gayatri Naik, " Visual Cryptography for Image Privacy", International Journal of Engineering and Technical Research (IJETR), ISSN: 2321-0869, Volume-3, Issue-3, March 2015.

[3] M. Naor and A. Shamir, "Visual cryptography," in EUROCRYPT, pp. 1–12, 1994.

[4] ching-nung yang and Chi-SungLaih,"New Colored Visual Secret Sharing Schemes", Journal of Designs, Codes and Cryptography, Vol.20, pp.325–335, 2000.

[5] Anusha and Subba Rao, "Visual Cryptography Schemes for Secret Image", International Journal of Engineering Research and Technology, Vol. 1, No. 5, pp. 1-9, 2012.

[6] G. Ateniese, C. Blundo, A. Santis & D. R. Stinson, "Extended capabilities for visual cryptography", ACM Theor. Comput. Sci., Vol.250,pp. 143-161,2001.

[7] E. R. Verheul & H.C.A. van Tilborg, Construction & properties of k out of n visual secret sharing schemes, Designs, codes & cryptography, vol.11, no. 2, pp.179-196, 1997.

[8] C. Chang, C. Tsai, and T. Chen. "A New Scheme For Sharing Secret Color Images In Computer Network", Proceedings of International Conference on Parallel and Distributed Systems, pp. 21–27, July 2000.

[9] Y. C. Hou, Visual cryptography for color images, Pattern Recognition, vol. 17773, pp.1-11, 2003.

[10] Ankita Gharat, Preeti Tambre, Yogini Thakare, Prof. S.M. Sangave, "Biometric Privacy Using Visual Cryptography", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 1, January 2013.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

[11] Arun Ross and Asem A. Othman," Visual Cryptography for Face Privacy", Proc. of SPIE Conference on Biometric Technology for Human Identification VII, (Orlando, USA), April 2010.

[12] Rahna. P. Muhammed," A Secured Approach to Visual Cryptographic Biometric Template", Proc. of Int. Conf. on Advances in Computer Engineering 2011.

[13] Divya James, Mintu Philip," A Novel Face Template Protection Scheme based on Chaos and Visual Cryptography", International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 2– No.5, May 2012.

[14] Biruntha.S , Dhanalakshmi.S," BIOMETRIC PRIVACY USING NON EXPANSIBLE VISUAL CRYPTOGRAPHY SCHEME", International Journal of Advanced Information Science and Technology (IJAIST), Vol.14, No.14, June 2013.