A Sophisticated Approach to Secret Sharing Using XOR with Authentication Using Iris Recognition

Smitha Joseph[a,*], Deepa S. Kumar[b] and Dr. M. Abdul Rahman[c]
[a,*] PG Scholar, College of Engineering, Munnar, Kerala, India.
josephsmitha33@gmail.com
[b] Research Scholar, Karpagam University, Coimbatore, India.
deepamsk@yahoo.com
[c] Pro Vice Chancellor, Kerala Technological University, Kerala, India.
pvc@ktu.edu.in

***Abstract*—Biometrics refers to technologies that measure and analyzes human body characteristics for authentication purposes. Iris recognition is a type of biometrics which use the features found in the iris to identify an individual. Visual cryptography is a cryptographic technique which hides information in images (called shares) that can be decrypted by human vision. Advanced hierarchical visual cryptography is a visual cryptographic technique used to improve the security which produces shares at different levels. For the authentication purpose, here the iris recognition is incorporated within the advanced hierarchical visual cryptography.**

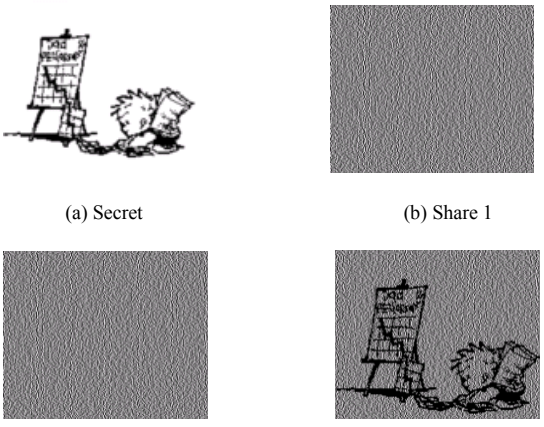
***Keywords*—Biometrics; Hamming distance; Hierarchical Visual Cryptography; Iris Recognition.**

I. INTRODUCTION

Visual cryptography (VC) is the art of encrypting information such as handwritten text and images in a perfectly secure way such that the decryption is possible without any mathematical computations and human visual system is sufficient to decrypt the information. The general idea behind visual cryptography technique is to divide the secret information into two shares and it demands both the shares while decrypting the information. Fig. 1 shows the basic visual cryptography scheme. Shares are printed on transparencies and then superimposed (i.e., logical X-OR operation is performed) to decrypt the secret. Each image holds different pieces of the original secret and when they are brought together the secret can be revealed very easily.

Hierarchical visual cryptography is a visual cryptographic technique in which the encryption of secret is performed at different levels thus improves the security. With some modifications to the hierarchical visual cryptography here, advanced hierarchical visual cryptography is used. The advantages of advanced hierarchical visual cryptography over hierarchical visual cryptography includes random generation of shares which decreases the complexity of share generation and less demand for memory since, the shares maintains the same size as that of the original secret [1].

Biometric technology deals with recognizing the identity of individuals based on their unique physical or behavioral characteristics. Physical characteristics such as fingerprint, palm print, hand geometry and iris patterns or behavioral characteristics such as typing pattern and handwritten signature present unique information about a person and can be used in authentication applications.



(a) Secret (b) Share 1

(c) Share 2 (d) Share1 + Share 2

Fig.1 Basic Visual Cryptography

The developments in science and technology have made it possible to use biometrics in applications where it is required to establish or confirm the identity of individuals. Applications such as passenger control in airports, access control in restricted areas, border control, database access and financial services are some of the examples where the biometric technology has been applied for more reliable identification and verification.

In recent years, biometric identity cards and passports have been issued in some countries based on iris, fingerprint and face recognition technologies to improve border control process and simplify passenger travel at the airports. In UK and Australia, biometric passports based on face recognition are being issued. The technology is designed to automatically take a picture from the passengers and match it to the digitized image stored in the biometric passports. Recently, US

Manuscript ID = 0001 - Copyright © 2015 International Computer Science and Engineering Society (ICSES), ISSN: 2467-292X
Website: www.i-cses.com --- E-mail: info@i-cses.com

government is also conducting a Registered Traveler Program which uses a combination of fingerprint and iris recognition technology to speed up the security check process at some airports. In the field of financial services, biometric technology has shown a great potential in offering more comfort to customers while increasing their security. As an example, banking services and payments based on biometrics are going to be much safer, faster and easier than the existing methods based on credit and debit cards. Proposed forms of payments such as pay and touch scheme based on fingerprint or smart cards with stored iris information on them are examples of such applications. Compared to passwords, biometric technologies offer more secure and comfortable accessibility and have dealt with problems such as forgetting or hacking passwords.

Iris patterns are formed by combined layers of pigmented epithelial cells, muscles for controlling the pupil, stromal layer consisting of connective tissue, blood vessels and an anterior 3 border layer. The physiological complexity of the organ results in the random patterns in iris, which are statistically unique and suitable for biometric measurements. In addition, iris patterns are stable over time and only minor changes happen to them throughout an individual's life. It is also an internal organ, located behind the cornea and aqueous humor, and well protected from the external environment. The characteristics such as being protected from the environment and having more reliable stability over time, compared to other popular biometrics, have well justified the ongoing research and investments on iris recognition by various researchers and industries around the world.

II. IRIS RECOGNITION

For iris recognition, Libor Masek method of recognition of Human Iris Patterns for Biometric Identification is used. The iris is an externally visible, yet protected organ whose unique epigenetic pattern remains stable throughout adult life. These characteristics make it very attractive for use as a biometric for identifying individuals. Image processing techniques can be employed to extract the unique iris pattern from a digitized image of the eye, and encode it into a biometric template, which can be stored in a database. This biometric template contains an objective mathematical representation of the unique information stored in the iris, and allows comparisons to be made between templates [10].

When a subject wishes to be identified by an iris recognition system, their eye is first photographed, and then a template created for their iris region. This template is then compared with the other templates stored in a database until either a matching template is found and the subject is identified, or no match is found and the subject remains unidentified. The system is to be composed of a number of sub-systems, which correspond to each stage of iris recognition [11]. These stages are segmentation – locating the iris region in an eye image, normalization – creating a dimensionally consistent representation of the iris region, and feature encoding – creating a template containing only the most discriminating features of the iris. The input to the system will be an eye image, and the output will be an iris template, which will provide a mathematical representation of the iris region.

A. Segmentation

It was decided to use circular Hough transform for detecting the iris and pupil boundaries. This involves first employing Canny edge detection to generate an edge map. Gradients were biased in the vertical direction for the outer iris/sclera boundary, as suggested by Wildes et al. Vertical and horizontal gradients were weighted equally for the inner iris/pupil boundary. The range of radius values to search for was set manually, depending on the database used. For the CASIA database, values of the iris radius range from 90 to 150 pixels, while the pupil radius ranges from 28 to 75 pixels. In order to make the circle detection process more efficient and accurate, the Hough transform for the iris/sclera boundary was performed first, then the Hough transform for the iris/pupil boundary was performed within the iris region, instead of the whole eye region, since the pupil is always within the iris region [9]. After this process was complete, six parameters are stored, the radius, and x and y centre coordinates for both circles.

B. Normalization

Once the iris region is successfully segmented from an eye image, the next stage is to transform the iris region so that it has fixed dimensions in order to allow comparisons. For normalization of iris regions a technique based on Daugman's rubber sheet model was employed. The centre of the pupil was considered as the reference point, and radial vectors pass through the iris region [8]. A number of data points are selected along each radial line and this is defined as the radial resolution. The number of radial lines going around the iris region is defined as the angular resolution. Since the pupil can be non-concentric to the iris, a remapping formula is needed to rescale points depending on the angle around the circle. This is given by:

$$r' = \sqrt{\alpha}\beta \pm \sqrt{\alpha\beta^2 - \alpha - r_1^2} \tag{1}$$

with

$$\alpha = o_x^2 + o_y^2 \tag{2}$$

$$\beta = \cos\left(\pi - \arctan\left(\frac{o_y}{o_x}\right) - \theta\right) \tag{3}$$

where displacement of the centre of the pupil relative to the centre of the iris is given by o_x, o_y and r' is the distance between the edge of the pupil and edge of the iris at an angle, θ around the region, and r_1 is the radius of the iris. The remapping formula first gives the radius of the iris region 'doughnut' as a function of the angle θ.

C. Feature encoding and Matching

Feature encoding was implemented by convolving the normalized iris pattern with 1D Log-Gabor wavelets. The

2D normalized pattern is broken up into a number of 1D signals, and then these 1D signals are convolved with 1D Gabor wavelets. The rows of the 2D normalized pattern are taken as the 1D signal; each row corresponds to a circular ring on the iris region. The angular direction is taken rather than the radial one, which corresponds to columns of the normalized pattern, since maximum independence occurs in the angular direction.

The encoding process produces a bitwise template containing a number of bits of information, and a corresponding noise mask which corresponds to corrupt areas within the iris pattern, and marks bits in the template as corrupt. Since the phase information will be meaningless at regions where the amplitude is zero, these regions are also marked in the noise mask. The total number of bits in the template will be the angular resolution times the radial resolution, times 2, times the number of filters used.

For matching, the Hamming distance was chosen as a metric for recognition, since bit-wise comparisons were necessary. The Hamming distance will be calculated using only the bits generated from the true iris region, and this modified Hamming distance formula is given as:

$$HD = \frac{1}{N - \sum_{k=1}^{N} Xn_k (OR) Yn_k} \sum_{j=1}^{N} X_j (XOR) Y_j (AND) Xn'_j (AND) Yn'_j \quad (4)$$

where X_j and Y_j are the two bit-wise templates to compare, Xn_j and Yn_j are the corresponding noise masks for X_j and Y_j and N is the number of bits represented by each template. Although, in theory, two iris templates generated from the same iris will have a Hamming distance of 0.0, in practice this will not occur. Normalization is not perfect, and also there will be some noise that goes undetected, so some variation will be present when comparing two intra-class iris templates.

In order to account for rotational inconsistencies, when the Hamming distance of two templates is calculated, one template is shifted left and right bit-wise and a number of Hamming distance values are calculated from successive shifts. This bit-wise shifting in the horizontal direction corresponds to rotation of the original iris region by an angle given by the angular resolution used. If an angular resolution of 180 is used, each shift will correspond to a rotation of 2 degrees in the iris region. This method is suggested by Daugman, and corrects for misalignments in the normalized iris pattern caused by rotational differences during imaging. From the calculated Hamming distance values, only the lowest is taken, since this corresponds to the best match between two templates.

III. PROPOSED METHOD

A. Advanced Hierarchical Visual Cryptography(AHVC)

In hierarchical visual cryptography (HVC), the secret is encrypted in a number of levels [1]. As the level of encryption in hierarchical visual cryptography increases, the secrecy tends to increase. For convenience, here we consider only two levels of encryption. That is, initially the secret is divided into exactly two shares called share1 and share2. Each of these shares are encrypted independently resulting in four shares: share11, share12, share21 and share22 [7].

Finally, HVC scheme gives two resultant shares out of which one is handed over to the user for authentication and another share is along with database [2]. The shares are generated using Noar and Shamir scheme, the two out of two visual cryptography. In the scheme stated here, a single pixel in original secret is represented by 2 pixels in the share. It gives raise to the expansion ration of 1:2. The basic algorithm for encrypting secret using HVC is given below.

(1) Begin
(2) Read original secret
(3) Encrypt secret using 2 out of 2 visual cryptography scheme (Share1 and share2 are generated here)
(4) Share1 is encrypted using 2 out of 2 visual cryptography scheme (Share11 and share12 are generated here)
(5) Share2 is encrypted using 2 out of 2 visual cryptography scheme (Share21 and share22 are generated here)
(6) Share12, share21 and share22 are combined to form key share
(7) Output remaining share, share11 and the key share
(8) End

Earlier each pixel in original secret is replaced by 4 pixels in share1 as well as in share2. Thus giving an expansion ratio of 1:4 [3]. The problem with both of these schemes is that, both demands more memory space since, as the level of encryption increases the size of the shares also tends to increase. So, we require an advanced hierarchical visual cryptographic scheme such that the size of shares remains the same as that of the original secret [5]. The benefit of reducing the expansion ratio is that the shares require less storage space over the server, reducing the time complexity of the authentication process.

The advanced hierarchical visual cryptography (AHVC) allows us to generate shares with the same size as that of the original secret with the same clarity which is analyzed using the correlation coefficient. Thus it demands only less storage space. In AHVC, first a random share i.e., the share1 is generated by taking any random value for each pixel. The requirement of this proposed method is that the secret should be in binary form. The random values for the pixels in the share will be 0 or 1 [6]. Then, the second share i.e., share2 is generated by XOR-ing every pixel of random share with every pixel of the original secret. When these shares, share1 and share2 are overlapped using the XOR operation, the result gives us the original image which will be the same as that of the original secret. Fig.2 shows the AHVC.

B. Algorithm for AHVC

Step 1: Random share (RS) generation, a random share is generated by taking any random value for each pixel (i.e., 0 or 1). The size of the share is same as the original image. Every time we create a random share it gives a different value for each pixel. So, no two random shares of the same image are same.

Step 2: Key share (KS) generation, a key share is generated by XORing every pixel of random share with every pixel of the original image. The size of this share is also same as the original image. No two key shares of the

same image are same since no two random shares are same.

Step 3: Overlapping of the shares is done by XORing the random share with the key share pixel by pixel. This results in the generation of the original image.

```
Algorithm AHVC ()
{
        For every pixel i=0 to n
        {
                RSi = B (0, 1)
                KSi = RSi ⊕ OIi
        }
        OI = RS ⊕ KS
}
/*OI= Original Image*/
```

C. Hierarchical Implementation of AHVC

The following steps describe the hierarchical implementation of advanced hierarchical visual cryptography.

Step 1: Select an input image

Step 2: Create two shares of the image called share1 and share2 using AHVC

Step 3: Share1 is the random share and share2 is the key share created by XORing original image with the random share.

Step 4: From share1 create share11 and share12 again using AHVC technique.

Step 5: Share11 is the random share and share12 is the XORing of share1 and share11.

Step 6: From share2 create share21 and share22 again using AHVC technique.

Step 7: Share21 is the random share and share22 is the XORing of share2 and share21.

Step 8: Select Share11 as the finalshare1.

Step 9: Create finalshare2 by XORing of share12, share21 and share 22.

To recover the original image we can overlap finalshare1 and finalshare2. The original image can also be recovered by overlapping share1 and share2. But overlapping of no intermediate shares: share11, share12, share21, share22 will reveal the image [4].

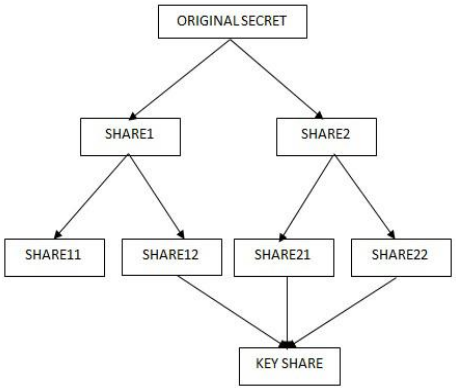


Fig. 2 AHVC

D. Authentication using iris recognition and AHVC

This proposed mechanism describes a safety authentication mechanism based on iris recognition and advanced hierarchical visual cryptography. The eye images used as the inputs are from the database of The Chinese Academy of Sciences – Institute of Automation (CASIA). Firstly, the biometric templates of the eye images are generated using the above mentioned Libor Masek method of Recognition of Human Iris Patterns for Biometric Identification. A biometric template is a digital reference of distinct characteristics that have been extracted from a biometric sample. These biometric templates are the inputs for the advanced hierarchical visual cryptography technique.

Here, for convenience two levels of encryption is performed. The templates are divided into shares are described above. One share is stored in the database along with user login and other given to user on ID card along with login. As the visual cryptography techniques guarantee that no information is revealed by one share alone, this provides security to the iris template in the database too.

For authentication user will provide share in the form of ID card. System finds the corresponding share from database. By stacking two shares iris feature template is generated. The new eye image supplied by user will be processed with three steps: segmentation, normalization and feature extraction which generates iris feature template of the new input. Then these two feature templates are matched using hamming distance. Thus authentication is performed using the value of hamming distance. The authentication process is shown in the Fig.3

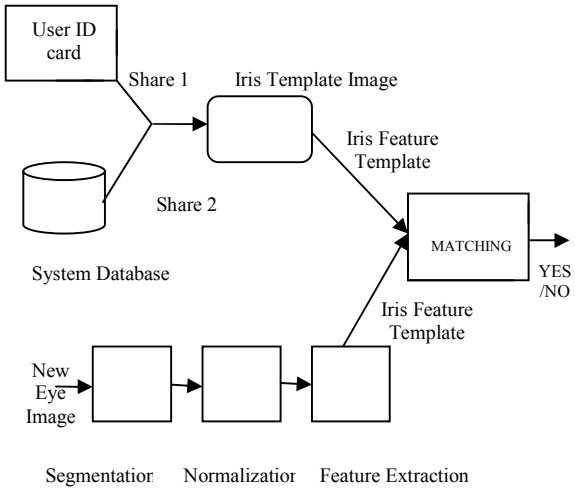


Fig. 3 User Authentication

IV. CONCLUSION

The authentication using iris recognition incorporated within advanced hierarchical visual cryptography could be a very useful mechanism in the security field. Since, the iris features of each one is unique, it will surely provide an excellent authentication system. And the advanced hierarchical visual cryptography provides share generation with the same size as that of the original secret. Earlier, the shares generated are expanded version of the original secret with expansion ration of 1:4 in first

experimentation. Later the expansion ratio is reduced to 1:2. And now this AHVC provides 1:1 ratio. The methodology of key share generation is defined with a set of three shares of original secret. The random share generation provides more security.

ACKNOWLEDGMENT

First and foremost, I would like to thank my Guides, Mrs. Deepa S. Kumar, Research Scholar, Karpagam University, Coimbatore and Dr. M. Abdul Rahman, Pro Vice Chancellor, Kerala Technological University for their valuable guidance and advice. Without their help this work would never have been completed.

I would like to thank all the teachers of the Computer Science Department of the college for providing me a good environment and facilities to do this work, without that, I would have faced many difficulties while doing this study.

Above all, I owe my gratitude to the Almighty for showering His abundant blessings upon me. And last but not the least I wish to thank my parents and my friends for helping me to do this work successfully.

REFERENCES

[1] P. V. Chavan and M. Atique, *Design of hierarchical visual cryptography*, in Engineering (NUiCONE), 2012 Nirma University International Conference on, pp. 13, IEEE, 2012.

[2] C. Hegde, S. Manu, P. Deepa Shenoy, K. Venugopal, and L. Patnaik, *Secure authentication using image processing and visual cryptography for banking applications*, *in Advanced Computing and Communications*, 2008. ADCOM 2008. 16th International Conference on, pp. 6572, IEEE, 2008.

[3] A. Shamir, *How to share a secret*, Communications of the ACM, vol. 22, no. 11, pp. 612613, 1979.

[4] P. Revenkar, A. Anjum, and W. Gandhare, *Survey of visual cryptography schemes*, International Journal of Security and Its Applications, vol. 4, no. 2, pp. 4956, 2010.

[5] T.-H. Chen, C.-S. Wu, and W.-B. Lee, *A novel subliminal channel found in visual cryptography and its application to image hiding*, *in Intelligent Infor- mation Hiding and Multimedia Signal Processing*, 2007. IIHMSP 2007. Third International Conference on, vol. 1, pp. 421424, IEEE, 2007.

[6] M. Naor and A. Shamir, *Visual cryptography, in Advances in Cryptology*EUROCRYPT94, pp. 112, Springer, 1995.

[7] C.-W. Lee and W.-H. Tsai, *Authentication of binary document images in png format based on a secret sharing technique*, in System Scienceand Engineering (ICSSE), 2010 International Conference on, pp. 506510, IEEE, 2010.

[8] Revenkar, P. S., Anisa Anjum, and W. Z. Gandhare. "Secure iris authentication using visual cryptography." *arXiv preprint arXiv:1004.1748* (2010).

[9] Njoroge, Kennedy N. "Iris detection for biometric identification." (2014).

[10] Mohammadi Arvacheh, Ehsan. "A study of segmentation and normalization for iris recognition systems." (2006).

[11] Masek, Libor. *Recognition of human iris patterns for biometric identification.* Diss. Master's thesis, University of Western Australia, 2003.