A.T. Hashim
Control and Systems Eng. Dept., Baghdad, Iraq
60102@uotechnology.edu.iq

D.A. Noori
Computer science Dept.
Baghdad, Iraq

Received on: 12/07/2016
Accepted on: 23/02/2017

Biometric Privacy Using Secret Image Sharing

Abstract- *Biometric technique includes uniquely identifying person based on their physical or behavioral characteristics. It is mainly used for authentication. Iris scanning is one of the most secure techniques among all biometrics because of its uniqueness and stability (i.e., no two persons in the world can have same iris). For authentication, the feature template in the database and the user template should be the same method for extracting iris template in this proposed system. Also storing the template in the database securely is not a secure approach, because it can be stolen or tampered. To deal with this security issue, the proposed system is securely storing the template in the database by firstly using randomness to scramble the bits of template based on chaos system. Secondly, a hiding technique is utilized to hide the scrambled templates in host images randomly. Finally, a secret sharing based on linear system is implemented on the iris template in database to protect it and adding extra layer of iris authentication system. The proposed secret sharing system has been generated a meaningful shares which overcomes the problem in traditional methods. Also in proposed system, two approaches of iris extraction have been presented.*

Keywords- *Iris Biometric, Feature extraction, Secret sharing, chaos system, Iris Authentication, hiding, random generator, GLCM, DWT*

How to cited this article: A.T. Hashim and D.A.Noori, "Biometric Privacy Using Secret Image Sharing," *Engineering and Technology Journal*, Vol. 35, Part A. No. 7, pp. ٧٠١-٧٠٨, 2017.

1. Introduction

Information technology world these days, system security is becoming very significant. Systems that using authentication are increasing because authentication have the main role to protect these systems from attackers. There are three types of authentication are "Password, card or token and biometric". It is easily to broken the password because the nature of human to make password easy to remember .Card or token can be stolen, there is no way to recognize the owner of it. Biometric provide secured method for identification and authentication, they are difficult to broken or replicated. Identity of biometric behavioral and physiological features is uses to authenticate identity of person. The work of biometric system is done by take and store information of biometric, then storing features are matching with the scanned biometric. One of the most typical and precise physiological features that can be used are irises [1]. A method that based on recognition of the random pattern of the iris in a biometric authentication system is called iris recognition. Iris recognition method is work by extract characteristics features of iris of individual's eye. Iris are uniqueness for every person, that, difference is exists between the eyes of the same person and even between the twins [2]. Biometric system can be considered as a regular system and the user can be easily deal with it. Biometric data and biometric system security have many issues until now. Centralized database is containing the template, but they are still under attack. So there are many mechanisms of protection can be used. For these reasons, many researches have been made using cryptography, stenography and watermarking in the system for the protection of biometric data and template [3].

This paper is portioned into Section 2 about the related work, section 3 about the proposed system, section 4 about the experiment results and finally section 5 about researcher paper.

2. Related Work

In 1993, John Daugman proposed an algorithm for iris recognition, the algorithm working by randomization the visible patterns in the iris of the eye to recognition the persons in real-time. He is uses in his algorithm for extract the structure of eye using a Gabor Wavelet Transform [4]. In 2010, Revenkar et al, applied visual cryptography to add extra layer of authentication for secure the iris template [5]. Alheeti in 2011, propose that many different steps for iris recognition are implemented, and uses many types of edge detection techniques [6]. In 2011, Kadim, uses Co-o.6ccurrence Matrix to extract features of the iris texture and then implemented this features in the K-means algorithm [7]. Chatterjee et al in 2013, proposed an active method for secure internet using iris recognition and cryptography, they uses Hough Transform for iris recognition [8]. Patil et al in 2013, proposed a system that divided template of fingerprint into different shares (two shares) with using visual cryptography techniques, keeping one with the identity person and the other one store in a database [9]. Thakur et al. in 2015, propose Gray-Level-Co-

https://doi.org/10.30684/etj.35.7A.5
2412-0758/University of Technology-Iraq, Baghdad, Iraq

occurrence Matrix for iris recognition by extract features of iris [10]. Kumar et al. in 2015, uses visual cryptography for dividing original image into different image but the shares image does not guide any information about original one, and for added more security by using asymmetric water marking [11]. Patil et al. in 2015 proposed that centralized database will be split by using secret sharing across different locations, this will reducing threats against centralized database and reducing the size of database [12].

In this paper, two approaches of iris recognition method have been proposed by applying GLCM (Gray Level Co-Occurrence Matrix) into the iris patterns and 2D Haar wavelet based method for extraction features. These features will be used for matching between stored features and the feature of tested iris. Then applying scrambling operation on this features for make the system more security. The proposed system used secret sharing method to increase security and privacy in iris based biometric system, a secret sharing method based on linear system, which is implemented on the iris template in database to protect it and adding extra layer of iris authentication system. The proposed secret sharing system has been generated a meaningful shares which overcomes the problem in traditional methods. The main purpose of this paper is the security of the iris template stored in the database.

3. Proposed System

One of the main challenges in the biometric system is the protection of the template, which is kept in database. Applying this system for only the authenticated user can access the secure resources.

The proposed system consists of two modules: Enrollment and Authentication, both are explained in the following subsections.

I. Enrolment Module

The database administrator captures and collects the eye image from the users who are authorized to access the secure resource. An enrolment module used for adding templates to a database. Enrollment module is subdividing into three sub modules: Generating templates module, generating shares module and hiding shares module. Figure 1 shows the components of the proposed enrolment module. An authorized person will have to pass through these phases as explained below.

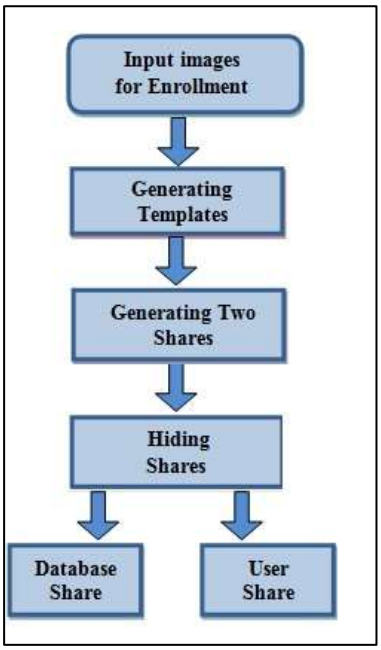

Figure 1: Enrolment Module

A. Generating Templates Module

For extraction the characteristics of the iris image, a feature extraction technique is applied, the extracted characteristics of the iris image are providing for enrolment and then it is stored in the database. The most distinguished information must be extracted for providing accurate recognition of individuals. The comparisons between templates can be made only if the significant features of the iris are encoded. The iris of human can be used for the recognition of the eye of one person from others because it is rich in features. In this paper, two methods have been used for feature extraction the first method based on co-occurrence matrix and second based on 2D wavelet transform. This paper uses publicly available Iris UBIRIS (**Noisy Visible Wavelength Iris Image Databases**) v1 session1 database.

1. Feature extraction based on co-occurrence matrix

Iris images are mapped into texture features produced from co-occurrence matrix where six features have been extracted for each iris. The color iris texture of size 32×128 is cut manually as shown in Figure 2. Then, algorithm 1 has been applied for extract the features of the iris based on co-occurrence matrix.

Figure 2: Sample of position and cutting iris texture

Image

ALGORITHM 1: GENERATING TEMPLATE BASED ON CO-OCCURRENCE MATRIX

Step1: Load iris texture image of size 32×128
Step2: Subdividing the cutting image into four blocks of size 32×32, then for each block**.**
Step3: Decompose block into R, G, and B bands
Step4: Convert R, G, and B color bands into HSI color components.
Step5: Applying a uniform color quantization (on H, S, and I color bands using following equation:

$$pixel(i,j) = \frac{pixel(i,j)}{255} \times Q \quad (1)$$

Where *Q* represents the quantization level
Step6: Construct a co-occurrence matrix for each band (i.e., quantized *H*, *S*, and *I*) with d = 1 and with four directions θ. where $\theta = (0^{\circ}, 45^{\circ}, 90^{\circ}, 135^{\circ})$.
This produces four matrices of (Q×Q) integer elements per matrix for each band.
Step 7: Normalize the resultant co-occurrence matrices by dividing each entry by the summation of all its entries.
Step8: Apply feature extraction for four normalized matrixes in four directions of band *I*. The following features have been extracted, where *p*(i, j) is the entry in normalized matrix [13]:
Step8-1: Apply Entropy Feature

$$Entropy = -\sum_{i,j} P(i,j) - \log P(i,j) \quad (2)$$

Step8-2: Apply Energy Feature

$$Energy = \sum_{i,j} P(i,j)^2 \quad (3)$$

Step8-3: Apply Inverse Difference Moment (IDM) Feature

$$IDM = \sum_{i,j} \frac{1}{1+(i-j)^2} P(i,j) \quad (4)$$

Step8-4: Apply Max Probability Feature

$$\text{Max Probability} = \text{Max}(P(i,j)) \quad (5)$$

Step8-5: apply Angular Second Moment Uniformity (ASMU)

$$ASMU = \sum_i \sum_j P(i,j) \quad (6)$$

Step8-6: Apply Inertia Feature

$$Inertia = \sum_{i,j} (i-j)^2 \; P(i,j) \quad (7)$$

This produces four matrices (4 features of Energy, 4 features of Entropy, …, and 4 features of Inertia) for each direction of *I* band .

Step9: Repeat step7 for normalized matrices of *S* and *H* bands.
Step10: Normalize the features by taking the average of each type feature as an example:

$$Energy_{total} = \text{Energy}_{0^{\circ}} + \text{Energy}_{45^{\circ}} + \text{Energy}_{90^{\circ}} + \text{Energy}_{135^{\circ}} / 4 \quad (8)$$

Step11: Apply the average normalization equation on the rest features. This gives six features for each band for each block.
Step12: Taking the average of features of four blocks. The resulted features in this stage are called iris code as a collection of 18 features (6 for each band).
Step13: Similarity Calculation
This stage is for matching between the new entered iris image and the image iris stored in database and making a decision about if it is found in data base or not. And the result of this stage is the identity of person.
Step13-1: Repeat the same stage of iris recognition and the same algorithms of enrollment stage.
Step13-2: Matching of the iris: finding the minimum distance classifier (MDC) in this step between the stored iris code and the iris code of the new iris image where MDC is:

$$\text{MDC} = \sqrt{\sum_{i=1}^{n} (V_{DB}(i) - V_{new}(i))^2} \quad (9)$$

Where: Iris Code= V (i.e. vector)
Step13-3: This step is about display the identity of person.

2. The extraction of features by using 2D Discrete Wavelet Transform (2D DWT)

Proposed system utilized Haar wavelet for feature extraction using five level decomposition techniques. After 5th level, vertical, horizontal coefficients of 4th level and 5th level have been combined , *i.e.*, LH4, HL4, LH5 and HL5 obtains feature vector of 40 elements because, it contains image pixel information which are sufficient for person identification efficiently The following Algorithm steps for feature extraction based on 2D DWT.

ALGORITHM 2: GENERATING TEMPLATE BASED ON 2D DWT

Step1: Load iris texture image of size 32×128

Step2: Convert R, G, and B color bands into Gray.
Step3: Apply 2D DWT with Haar up to 5-level decomposition.
Step4: Using the HL and LH details of 4th level and 5th level decomposition for constructing the feature vectors.
Step5: The resulted features in this stage are called iris code as a collection of 40 features which have been stored in feature vectors in database.
Step6: Similarity Calculation
This stage is for matching between the new entered iris image and the image iris stored in database and making a decision about if it is found in data base or not. And the result of this stage is the identity of person.
Step6-1: Repeat the same stage of iris recognition and the same algorithms of enrollment stage.
Step6-2: calculating hamming distance for each image feature vector using equation (9), then Finally Calculate minimum Hamming Distance.
Step6-3: This step is about display the identity of person.
Figure 3 shows the results of coefficient and the level of first decomposed image like coefficient of approximation, first coefficient of vertical, coefficient of horizontal and coefficient of diagonal , the first decomposed image size are 16×64 pixels. In similar way the second level decomposed approximation has size 8×32 for vertical, horizontal and diagonal specifics. In third level of decomposed approximation has size 4× 16 for vertical, horizontal and diagonal specifics. In forth level of decomposed parataxis has size 2×8 for vertical, horizontal and diagonal specifics. At last, fifth level of decomposed approximation has size 1×4 for vertical, horizontal and diagonal specifics. Now takes the core of the iris pattern, which represents the coefficients. Then that detect redundant information must be discarded. Actually, most of the patterns in the cD_1^h, cD_2^h, cD_3^h, cD_4^h, are the same and can choose one of them to discard redundancy. Since cD_4^h has the smallest size and it is duplicate the same patterns as preceding horizontal level, therefore takes it as a delegate of all information the four levels carry. The fifth level must be selected as a whole for this reason that it does not have the same textures. In a similar process, the characteristic patterns in the iris-mapped image can represent by chosen only fourth and fifth vertical coefficient. This represents that each image applied to the Haar wavelet as the collection of four matrices i.e. cD_4^h, cD_5^h, cD_4^v, cD_5^v. These matrices are collected to build one single vector characterizing the iris patterns. Such vector is called Feature vector.

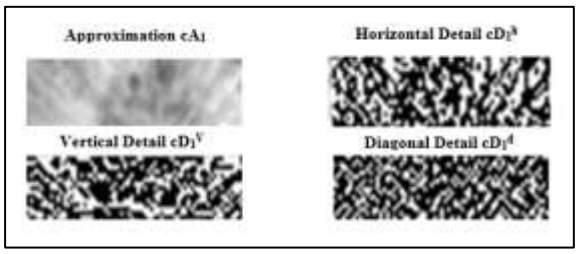

Figure 3: 1st level Haar decomposition in terms of cA1,cD_1^h, cD_1^V, cD_1^d

B. Generating Two Shares
The proposed secret sharing allows us to encode a secret template (i.e., list of features) into two shares. These shares appear as a random set of pixels. The shares could be reformulated as natural images –known as host images in the next step where each share is hiding into fixed host image.
The proposed system has been used (2, 2) secret sharing based on linear system adaptive from [14] for generation shares. At first the template bits have been scrambled randomly based on chaotic system then, it is decomposed into two shares These share templates has been hidden in two different host meaningful images, and one of them is kept with user on card ID and other is kept in the database. The iris template security is provided because no information can be retrieved for the enrolled eye by using the only one share, which is kept in the database. During reconstruction phase, these images are fetched and stacked together to get original template. Algorithm (3) illustrates the generating shares steps.

ALGORITHM 3: GENERATING TWO SHARES
Input: Features // list of iris features
Output: S1, S2// two shares
Step1: Mapping the negative features into positive.
Step2: Convert iris features into binary to generate binary stream called template of length *L*.
Step3: Generate Random sequence of length *L* based on logistic map system using Algorithm (5).
Step4: Randomize the positions of bits in template itself using random sequence generated in step 3.

Step5: Convert the resultant binary sequence to decimal to generate a sequence of integer numbers for each template.
Step6: Take block (i.e., two numbers) from generated sequence of integers called b1 and b2.
Step7: Apply linear system for all blocks of host image to generate two shares. The sharing system is based on using two of linear equations such that each i^{th} share has a secret set of two integer numbers, k_{ij} (where, $i \in [1,2]$ and $j \in [1,2]$). In other words, for two integer numbers b1 and b2 and two bytes sub key k1and k2 which are associated with each shares calculate S1 and S2 using the following linear system:

$$S1 = (k1b1 + k2b2) \bmod 256 \quad (10)$$

$$S2 = (k3b3) + (k4b4) mod\ 256 \quad (11)$$

Where S1 and S2 are two generated shares.

C. Hiding Shares

The proposed system has been combined the ability of scrambling the template bits randomly based on chaotic system and hiding generating shares, in some cover image randomly which are provided by administrator to maintain security (see Figure 4). The LSB (Least Significant Bit) technique is the simplest technique of hiding insertion. If specifically consider still images, each pixel of the color image has three components -- red, green and blue. Then, each color has 8 bits, in which the intensity of that color can be specified on a scale of 0 to255.Thus, for every third byte of each pixel of third byte (i.e., blue component) can be used to hide one bit of template. An algorithm for hiding shares would be shown in the following algorithm:

ALGORITHM 4: HIDING TEMPLATE
Input: S1, S2, // two shares (i.e., two arrays of integer numbers)
Two Host images, // provided by administrator
W, H // width and height of host image
Key1, Key2 // two keys for chaotic system
Output: Two StegoImages
Step1: Convert the generating two shares into two binary sequences of length *L1* and *L2* respectively**.**
Step2: Take Key1 and Key2 and generate two random sequences *R1* and *R2* of length *L1* and *L2* respectively based on logistic map system using Algorithm (5).
Step3: Hide each binary sequence in host image randomly using random sequence generated in step 2. The Algorithm (6) has been utilized for hiding.

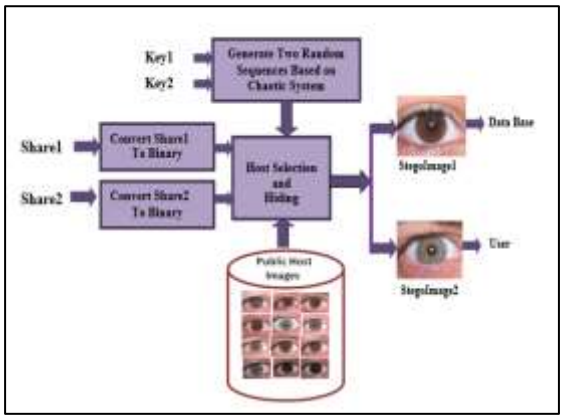

Figure.4: Hiding Shares

ALGORITHM 5: RANDOM DENERATOR BASED ON LOGISITICMAP SYSTEM
Input: r_min, r_max, num_intervals, // initial values
L // Length of sequence;
Output: R // random sequence
Step1: Set r_min = 3.0, r_max = 4.0, num_intervals = 21.
Step2: Initialization for random generator, srand (time(NULL))
Step3: Set r= r_min, m=0

```
FOR I = 0 to num_intervals
  Begin
    r = r+ (r_max - r_min) / num_intervals
    X= rand () / RAND_MAX
      FOR j=0 to L
        Begin
          x_n = r × x × (1-x)
          y = (x_n×1000) mod L;
          If (not found in R)
            Begin
              R[m] = y
                m = m+1
            Endif
          If (m > L)
                Exit ()
          EndIf
      EndFor
EndFor
```

ALGORITHM 6: HIDING TEMPLATE
Input: S1, S2 // Two Shares
L1, L2 // length of shares S1, S2 respectively
HostImage1, HostImage2 // Two host images
W, H // width and height of host images
R1, R2 // Two random sequences
Output: Two StegoImages
Step1: Set m=0

```
For i=2 to W*H*3 step 3
    If (m < L1)
        Begin
```

```
                bit= S1[m]
              m=m+1
              if ( bit = 1 )
 HostImage1[R[i]]=HostImage1 [R[i]] OR 0x01
                    Else
 HostImage1[R[i]]=HostImage1  [R[i]]  AND
0xFE
                Endif
          Else
               Break
     End For
```

Step2: Repeat Step1 with HostImage2, L2 and R2 for hide S2.

II. Authentication Module

The meaningful share in the form of the identification (ID card) will provide the user authentication and the corresponding meaningful share from the database will the system find it. To extract template, would simply need to take the data in the LSBs of the random color bytes using the same random sequence that is used in enrollment stage and combine them. Then the template bits rescrambled by using the same random sequence that is used in enrollment stage. By using the (2, 2)/Threshold reveal phase of linear system [14], the iris template is generated from two shares. The new eye image provided by user will be processed with the same steps of generating template in enrollment model for generating feature template of the iris. Then matching the two feature templates by using hamming distance. If features match access is granted, else the verification fails. Figure 5 shows the authentication module.

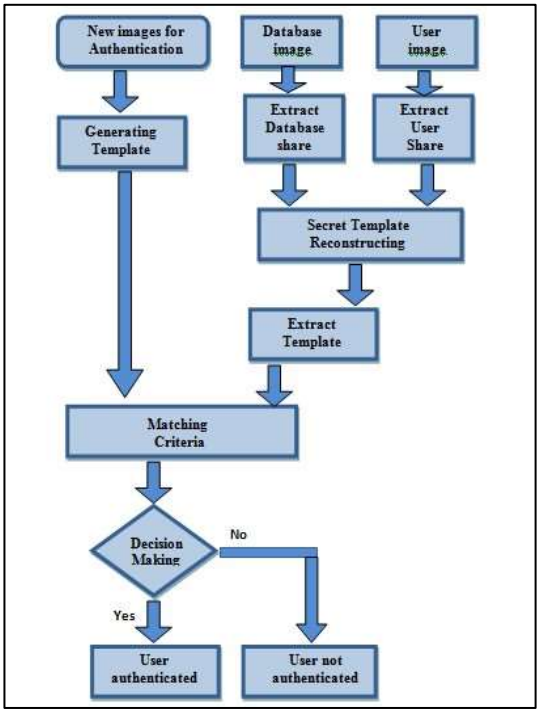

Figure 5: Authentication module

4. Experiments Results

The algorithms of image processing are proposed by extracting the features of the iris. Visual C++ platform is used to build this system. This paper uses publicly available Iris UBIRIS v1 session1 database comprised of 1173 images collected from 241 subjects within the University of Beira Interior 6. In this paper, 482 images are taken (i.e., 241 images for test and 241 for enrollment for all persons in database.). The image size has been reduced to (width, height) = (400, 300) this process allowed us still enough quality for the execution of the algorithms. Figure 6 illustrates some of the noise factors that images of the UBIRIS database contain. Within non-cooperative image capturing environments, it is highly expectable to capture poor focused images iris obstructed by eyelids and eyelashes specular and lighting reflections in the iris regions, motion blurred images or even images without any visible portion of the iris.

All the images in session1 are manually classified with respect to three parameters ('Focus', 'Reflections' and 'Visible Iris') are scaled into ('Good', 'Average' and 'Bad'). This classification is given in table 1 and confirms without doubt the variability of the images quality according to the capturing session [15].

The proposed system considers Haar wavelet and co-occurrence matrix for feature extraction and found Haar is more efficient as compared to co-occurrence matrix with less computational time as shown in as in table 2 and table 3. Experiment is carried using Haar wavelet with 5-level decomposition for feature extraction. Figure 7 shows the conceptual diagram for organizing feature vector by five level decomposition of normalized image.

Figure 6: Examples of images from the UBIRIS database

Table 1: Classification of UBIRIS images quality, regarding focus, reflections and proportion of visible iris, according to the image capturing session

Parameter	Good, %	Average,%	Bad,%
Focus	76.10	16.51	7.39
Reflections	78.52	19.09	1.99
Visible Iris	43.65	52.86	3.49

Table2: Comparison of proposed two methods result using recognition Accuracy criteria for the UBIRIS database for cooperative environment

Methods	Normalized size	No of Images	Feature Vector	Accuracy
2D DWT	32×128	482	40	95.67
Co-occurrence matrix	32×128	482	18	70.50

Table3: Time Computational Complexity Cost for Feature Extraction

Methods	No of Images	Quantization step	Feature Extraction in Sec.
2D DWT	241	-	1.04
Co-occurrence matrix	241	8	17.44

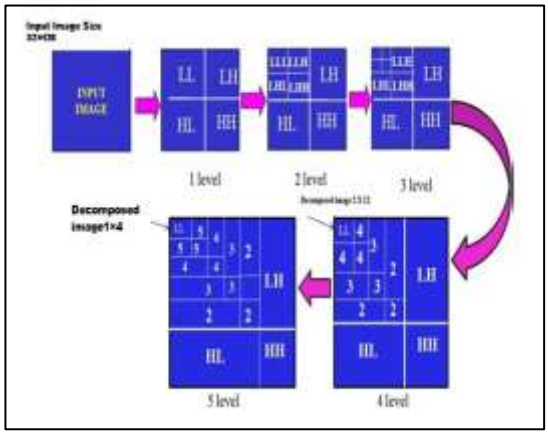

Figure 7: Five level decomposition of cutting iris texture image

Figure 8 and figure 9 show the implementation of enrollment and authentication steps respectively.

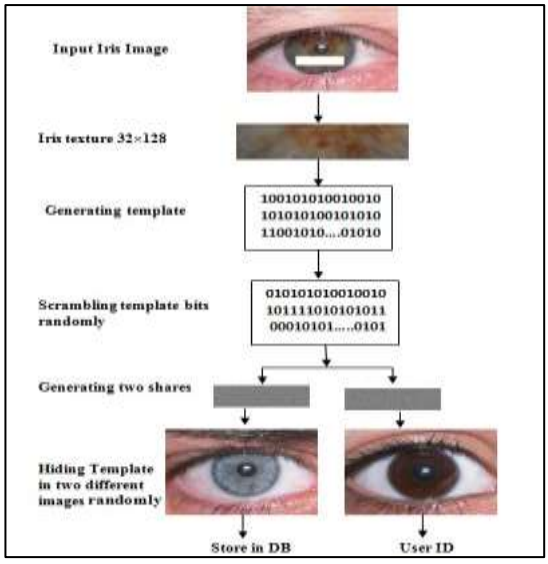

Figure 8: The implementation of enrollment steps

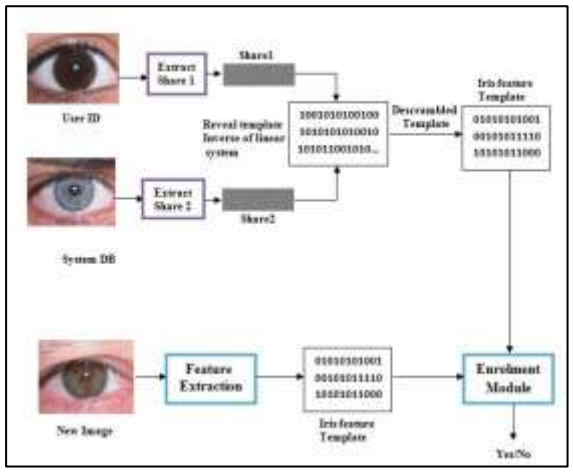

Figure 9: The implementation of authentication steps.

5. Conclusions

The proposed system secret sharing technique is used for the iris template protection stored in database and provided more layer of authentication for the existing iris authentication system. As enrolled iris template has been performed feature extraction using two methods the first is based on 2D DWT and the other based on the co-occurrence matrix. In order to reduce errors and achieve good accuracy, the proposed system is considered lower half of iris part for features extraction. Then the template is divided into two shares using secret sharing one is kept in the database as a meaningful image after template has been hidden randomly and other with user as the ID card. The iris template security is provided because no information can be retrieved for the enrolled eye by using the one share which is kept in the database. In this case access from unauthorized user is avoided. This system will be more secure and reliable in security-critical applications.

References

[1] P. Khaw, "Iris Recognition Technology for Improved Authentication," SANS Security Essentials (GSEC) Practical Assignment, Version 1.3, 2002.

[2] L. Masek, "Recognition of Human Iris Patterns for Biometric Authentication," This report is submitted as partial fulfilment of the requirements for the Bachelor of Engineering degree of the School of Computer Science and Software Engineering, The University of Western Australia, 2003.

[3] P.S. Revenkar, A. Anjum and W.Z. Gandhare, "Secure Iris Authentication Using Visual Cryptograph," (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No.3, 2010.

[4] J.G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 25, No. 11, Pp. 1148-1161, 1993.

[5] P.S. Revenkar, A. Anjum and W.Z. Gandhare, "Secure Iris Authentication Using Visual

Cryptography," (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No.3, 2010.
[6] K.M. Ali Alheeti, "Biometric Iris Recognition Based on Hybrid Technique," International Journal on Soft Computing (IJSC) Vol.2, No.4, November 2011.
[7] A.M. Kadim, "Iris Texture Recognition Using Co-occurrence Matrix Features with K_means Algorithm," Journal of Al-Nahrain University, Vol. 14, 4, December, pp.185-190, 2011.
[8] K. Chatterjee, N. Mrinal and Prasannjit, "An Efficient Implementation of Iris Recognition and Cryptography in Internet Security System," IJCA Special Issue on "Recent Trends in Pattern Recognition and Image Analysis" RTPRIA, 2013.
[9] S. Patil, K. Tajane and J. Sirdeshpande, "SECRET SHARING SCHEMES FOR SECURE BIOMETRIC AUTHENTICATION," International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013.
[10] S. Thakur, S. Rana and V. Thakur, "Biometric Security Enhancement using GLCM Method: A Review," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 4, Issue 5, May 2015.
[11] S.K., Manu K.Y. Reshma Pawar and M. Patil, "Security Using Biometrics Template And Visual Cryptography: A Two Fold Approach," International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS) Volume 2, Issue1, Jan-Feb 2015.
[12] R.S. Patil, S. Patil and S.D. Thepade, "Secret Sharing based Secure Authentication System," International Journal of Computer Applications (0975 – 8887) Volume 118 – No.22, May 2015.
[13] P. Mohanaiah, P. Sathyanarayana and L. GuruKumar, "Image Texture Feature Extraction Using G LCM Approach," International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013.
[14] A.T. Hashim and L.E. George, "Secret Image Sharing based on Wavelet Transform," Elsevier Science and Technology Series book, Advances in Engineering and Technology Series, Pp. 443- 451, 2013.
[15] H. Proenc¸a and Lu´ıs A. Alexandre, "Ubiris iris image database," 2004. http://iris.di.ubi.pt

Author(s) biography

Ashwaq T. Hashim is working as Assistant Professor in Control and Systems Engineering Department, University of Technology, Iraq. She obtained M.Sc. from computer science/ University of Basrah in 2003 and Ph.D. from University of Babylon in 2014. She published more than 22 papers in cryptography, image processing and VHDL.

Duaa A.Noori is a master student in Computer Science Department, University of Technology, Iraq. She is having her B.Sc. from Computer science / University of Technology in 2014.