Improvisation of Template Protection in Iris Biometric Recognition using Watermarking Technology

K. Sambasivarao, M.tech Student, Department of Electronics and Communication, Engineering. S.R.K.Institute of Technology, Enikepadu, Vijayawada
T. Vishnu Priya, Asst.Professor, Department of Electronics and Communication, Engineering. S.R.K.Institute of Technology, Enikepadu, Vijayawada

ABSTRACT

Biometric recognition is noteworthy method for recognition of person in recent years. The aim of our biometric recognition system is to improve the template protection by embedding the iris data to hand vein images based on watermarking technology. In order to handle this issue, researches have proposed different algorithms to be confronted by security of biometric systems. Two major ways are, (1) Encryption, and (2) watermarking by securing biometric images and templates. In this project, we utilize a watermarking technology to improve the template security in biometric authentication. According to, two modalities such as, iris and hand vein is taken to preserve the characteristics of liveliness and permanency. The existing technique of embedding of iris data to hand vein images using watermarking technology consist of following steps, i) preprocessing of iris and hand vein images, ii) iris template extraction, iii) Vein extraction, iv) Embedding of iris pattern to vein images based on region of interest, v) Storing embedded images. After this the extracted iris template was embedded in to the hand vein and stored in the database. Subsequently in recognition phase the iris template and hand vein features were extracted from the watermarked image. Finally the extracted features were matched with input query image. The final decision of authentication was done based on the product rule-based score level fusion. The implementation is done using MATLAB and the performance of the technique is analyzed with FAR, FRR and accuracy. The proposed method can be further improving the Accuracy by considering the embedding the iris data to fingerprint images using watermarking technology for template protection.

Keywords

Authentication, Embedding and Extraction, Fingerprint, Template, Watermarking.

1. INTRODUCTION

Biometric system, which is a pattern recognition system, exploits a user's inimitable physical traits to identify/ authenticate him/her [1]. Two major groups of tasks that contribute in a biometric system are identification and authentication [2]. The growing ubiquity of smart phones has accelerated their use in Internet applications. The daily usage of mobile devices with Internet access has enabled online businesses to use them for identification purposes. For instance, a mobile device can receive a short message verification code called one-time password which is used for online banking authentication. Biometric techniques considers numerous traits such as facial thermo gram, hand vein, gait, keystroke, odor, ear, fingerprint, face, hand geometry, retina, palm print, iris, voice and signature [3].

Iris recognition works on the basis of visual features such as rings, freckles, furrows and corona. Due to the high degree of randomness in such features, iris recognition is found to be very challenging. This leads research concepts in hand vein recognition as one of hot spot areas in biometric authentication. Patterns available in the hand veins are found to be distinctive between the individuals and remain same for long term throughout the human life. From the literature survey, [2], [3], [4], [5], [6] the researchers had discussed about various template security method and their importance in security of biometric template protection. Also, we found that there is need of robust biometric recognition technique for template protection. So here we design a biometric recognition system by embedding iris data to hand vein images using watermarking technology. The range of biometric modalities (i.e. iris, fingerprint, hand vein), fingerprints have been the most widely used in authentication systems due to their uniqueness, immutability and convenience [7].First, fake fingerprint images can be constructed easily

using several spoofing approaches to accessing a system [8]. Second, the original fingerprint sample used in one application can be tampered with; therefore, all other applications using the same sample may have problems due to the fact that fingerprint features cannot be replaced or cancelled. To overcome the above issues, watermarking can be used to verify the authenticity of a fingerprint sample. This paper investigates different digital watermarking techniques to prove the genuineness of fingerprint image.

2. EXISTING METHOD OF EMBEDDING IRIS DATA TO HAND VEIN IMAGES USING WATERMARKING TECHNOLOGY

The aim of our biometric recognition system is to improve the template protection by embedding the iris data to hand vein images based on watermarking technology. The existing technique of embedding of iris data to hand vein images using watermarking technology consist of following steps, i) preprocessing of iris and hand vein images, ii) iris template extraction, iii) Vein extraction, iv) Embedding of iris pattern to vein images based on region of interest, v) Storing embedded images.

2.1 Iris Image Pre-processing and key generation

The initial stage of our existing method is pre-processing in which the iris images are acquired and process to extract the iris key. By subsequent localization, the information related with iris part is selected from the entire image.

2.1.1 Iris Localization

The first stage of iris recognition is to isolate the actual iris region in a digital eye image. The iris region can be approximated by two circles, one for the iris/sclera boundary and another, interior to the first, for the iris/pupil boundary. The eyelids and eyelashes normally occlude the upper and lower parts of the iris region. Also, specular reflections can occur within the iris region corrupting the iris pattern. Boundaries of the iris and the pupil are determined to perform edge detection process. These boundaries and radii can be determined by integro-differential operator proposed by Daugman. It is given in equation (1) as:

$$\max(r,a_0,b_0)\,|\,G_\sigma(r)*\frac{\partial}{\partial r}\oint r,a_0,b_0\,\frac{I(a,b)}{2\pi r}ds\,| \tag{1}$$

The aforesaid operator searches the gradient image along with boundary of circles with high radii and hence it behaves as a circular edge detector.

2.1.2 Image 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. The normalization process will produce iris regions, which have the same constant dimensions, so that two photographs of the same iris under different conditions will have characteristic features at the same spatial location. This can be done using Daugman's rubber sheet model. According to the base paper analysis equations

$$R' = \sqrt{\alpha\beta} \pm \sqrt{\alpha\beta^2} - \alpha - R_1^2 \tag{2}$$

Where, R_1 represents iris radius.

$$\alpha = a_x^2 + b_y^2$$

$$\beta = \cos\left(\pi - \arctan\left(\frac{b_y}{a_x}\right) - \theta\right)$$

Radial resolution and angular resolution of the image are set to 100 and 2400, respectively.

2.1.3 Encoding

In order to provide accurate recognition of individuals, the most discriminating information present in an iris pattern must be extracted. Only the significant features of the iris must be encoded so that comparisons between templates can be made. Most iris recognition systems make use of a band pass decomposition of the iris image to create a biometric template.

According to the base paper analysis equations:

$$H\{R_e, I_m\} = \mathrm{sgn}\{R_e, I_m\}\int_\rho\int_\phi I(\rho,\phi)e^{-i\omega(\theta_0-\phi)}e^{-(r_0-\rho)^2/\alpha^2}e^{-(\theta_0-\phi)^2/\beta^2}\rho d\rho d\phi \tag{3}$$

Log Gabor filter can be represented as in equation (4) below

$$G(f) = \exp\left(\frac{= (\log(f / f_0))^2}{2(\log(\sigma / f_0))^2} \right) \quad (4)$$

Gabor - convolve function results in complex value convolution output with size similar that of the size of input Image.

2.2 Hand Vein image pre-processing and feature extraction

In this the dorsal hand vein images are acquired by an array of infrared light-emitting diode (LED) and a thermal camera. Further to reduce the noise, the obtained hand vein image is pre-processed initially. Then apply mask to the pre-processed hand vein image. The size of the image obtained after masking is same as the input. After this the blood vessels from the hand vein image are obtained by using kirsch's template extraction method. According to the base paper analysis equations.

$$K_{a,b} = Max_{d=1...8} \sum_{n=-1}^{1} \sum_{m=-1}^{1} W_{nm}^{(d)} . p_{a+n,b+m} \quad (5)$$

Were d is the 8 direction as given below,

$$d = \{W^{(1)}, W^{(2)}, W^{(3)}, ...W^{(8)}\}$$

$$T(x,y) = m(x,y) + c \times v(x,y) \quad (6)$$

Where, T(x,y) is the threshold, C is the coefficient of correction.

Mean $$m(x,y) = \frac{1}{r^2} \sum_{i=x-r/2}^{x+r/2} \sum_{j=y-r/2}^{y+r/2} f(i,j) \quad (7)$$

And

Variance $$v(x,y) = \sqrt{\frac{1}{r^2} \sum_{i=x-r/2}^{x+r/2} \sum_{j=y-r/2}^{y+r/2} f^2(i,j)} \quad (8)$$

L = 0.97 x Length of the blood vessel obtained (9)

Then choose the obtained pixel value as a threshold. Finally the pixel value below the threshold is selected as the features of the hand vein.

2.3 Embedding of iris pattern to band vein image

The input is iris key image l(x,y) and the watermark image is the hand vein image H(x,y). The output is the watermarked image H w (x, y) .

The various steps in watermark embedding is

l) The input watermark image H(x,y)is divided into blocks of size B_1,B_2, B_3 .....B_n of size MxN. Then the divided block is sorted. From the sorted block of the input image H(x,y) the first wavelet coefficient with positive phase and the value below the threshold T(x,y) is chosen.

2) Then the second LSB of the selected block of the watermark image H(x,y)is replaced by one bit from the iris template I(x,y). This process is shown below in equation (11),

$$C'_W(x,y) = \{ LSB(C_W(x,y) = I(x,y) if phase(C_W(x,y)) \geq 0 \,\&\, C_W(x,y) < T(x,y)$$

$$C_w(x,y) if phase(C_w(x,y)) < 0 \quad (10)$$

Where, C_W(x,y)is the coefficient in block B_n. Here T(x,y) is the threshold whether the watermark bit is inserted or not.

3) If the number of bits in the iris template I(x,y) is less than the number of blocks in hand vein image, then all bits of the iris template I(x,y) can be embedded.

4) After embedding all the bit of the iris template I(x,y) in hand vein image an IDWT (Inverse Discrete Wavelet Transform) is applied to the watermarked hand vein coefficient to generate the final secure watermarked hand vein image. The watermark embedding process is shown in the figure below.

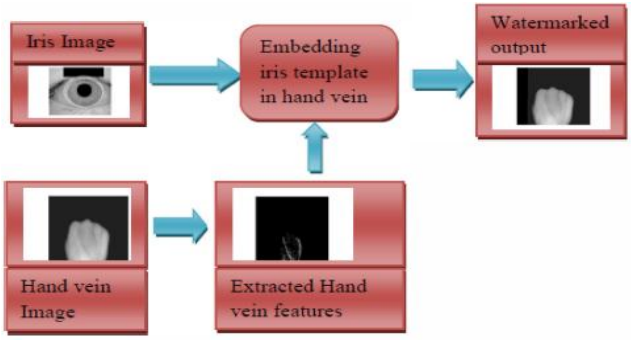

Fig. 1. Watermark Embedding

2.4 Recognition Phase using Score level fusion

The recognition phase is divided in two major steps.

2.4.1 Watermark extraction

In this recognition phase the watermarked image is given as input and the iris key and hand vein features are extracted. The watermark extraction phase consists of various steps. The input is watermarked image $H_w(x,y)$ and the size of watermarked image $H_s(x,y)$ and the output is recovered watermark image $R_w(x, y)$.

1) The watermarked image is divided in to the detail sub band of watermarked image in to blocks. The each block of the watermarked image is of size 2M -1 x 2N -1.

2) Identify the value below the threshold T(x,y) in each block which has the first coefficient with positive phase.

3) The pixel value 1 from the watermarked image is extracted if the embedded pixel value is greater than the mean pixel value otherwise pixel value '0' is extracted. This process is repeated until all the pixels from the watermarked image are y given in equation (12) below

$$H'_s(x,y)=\{1, B_{(i)}>B_n, 0<i<n \quad (11)$$

$$0, \text{otherwise}$$

4) A matrix equal to the size of watermark image Hw(x,y) and the extracted pixels are placed in it to obtain the watermark image $H_s'(x,y)$.

In recognition phase the both iris and vein image of an individual is taken. Then both the obtained iris image and the hand vein image are pre-processed separately as by the above procedures. So here we have to extract the iris key and vein image separately.

2.4.2 Matching

The matching distance for the input iris key and the extracted iris key from embedded image is denoted as D_{iris}. Likewise the pre-processed vein image of the same person is matched with the vein image feature extracted from the embedded image stored in database. Finally a matching distance D_{vein} for the vein image is determined. Further the two normalized similarity distance D_{iris} and D_{vein} are fused linearly using sum rule as given in equation (12) below,

$$MS = \alpha * D_{iris} + \beta * D_{vein} \quad (12)$$

Where α and β are two weight values that can be determined using some function. In this paper a combination of linear and exponential function is used. The value of MS is used as the matching score. So if matching score is greater than threshold value then individual is allowed to enter the system otherwise rejected.

3. PROPOSED EMBEDDING IRIS DATA TO FINGERPRINT IMAGES USING WATERMARKING TECHNOLOGY

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify an individual and verify their identity. Because of their uniqueness and consistency over time, fingerprints have been used for over a century, more recently becoming automated (i.e. a biometric) due to advancement in computing capabilities. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration.

i) Fingerprint Recognition

ii) Fingerprint Patterns

iii) Embedding Of Iris Pattern to Fingerprint Image

iv) Watermark Extraction

3.1 Fingerprint Recognition

Human fingerprints have been discovered on a large number of archeological artifacts and histological items.

Although these findings provide evidence to show that ancient people were aware of the individuality of fingerprints, it was not until the late sixteenth century that the modern scientific fingerprint technique was first initiated (Jain, et al, 2003). Every person's fingerprints are unique, and will always maintain their uniqueness explaining why they have been used for many years for authentication purposes. For example, the FBI fingerprint identification division was set up, in 1924, with a database of 810,000 fingerprint cards (Federal Bureau of Investigation, 1984).In 1890, Alphonse Bertillon studied body mechanics and measurements to help in identifying criminals.

3.2 Fingerprint Patterns

A fingerprint consists of three basic patterns of ridges, the arch, loop and whorl as shown in Figure 2. An arch can be explained as the pattern where ridges begin from one side of the finger, ascent in the centre which develops an arc, and then exits the finger from the opposite side. A loop can be explained as the pattern where ridges begin at one side of a finger to create a curve, and are inclined to exit in the same way they entered.

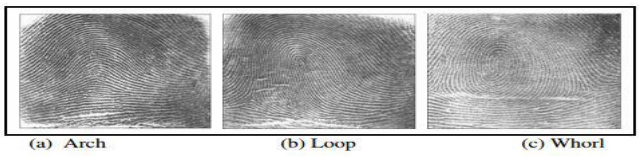

Fig. 2. Basic Patterns of Fingerprint

As seen above in Figure 2(c), in the whorl pattern, ridges are structured in a circular position around a central spot on the finger. In general, researchers have discovered that relatives frequently share similar fingerprint patterns, which has led to the concept that fingerprint patterns are genetic.

3.3 Embedding of Iris Pattern to Fingerprint Image

l) The input watermark image F(x,y)is divided into blocks of B_1,B_2,B_3, ...B_n of size MxN. Then the divided block is sorted. From the sorted block of the input image F(x,y) the first wavelet coefficient with positive phase and the value below the threshold T(x,y) is chosen.

2) Then the second LSB of the selected block of the watermark image F(x,y)is replaced by one bit from the iris template I(x,y).

3) If the number of bits in the iris template I(x,y) is less than the number of blocks in fingerprint image, then all bits of the iris template I(x,y) can be embedded.

4) After embedding all the bit of the iris template I(x,y) in fingerprint image an IDWT (Inverse Discrete Wavelet Transform) is applied to the watermarked fingerprint coefficient to generate the final secure watermarked fingerprint image. The watermark embedding process is shown in the figure below,

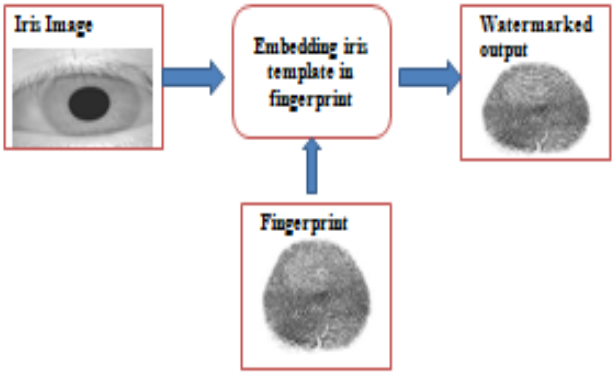

Fig. 3. Fingerprint watermark Embedding

3.4 Watermark Extraction

The watermark extraction phase consists of various steps:-

The input is watermarked image $F_W(x,y)$ and the size of watermarked image $F_S(x,y)$ and the output is recovered watermark image R_W (x, y).

1) The watermarked image is divided in to the detail sub band of watermarked image in to blocks. The each block of the watermarked image is of size 2M -1 x 2N -1 .

2) Identify the value below the threshold T(x,y) in each block which has the first coefficient with positive phase.

3) The pixel value 1 from the watermarked image is extracted if the embedded pixel value is greater than the mean pixel value otherwise pixel value '0' is extracted.

4) A matrix equal to the size of watermark image $F_W(x,y)$ and the extracted pixels are placed in it to obtain the watermark image F_s' (x,y) .

In recognition phase the both iris and fingerprint image of an individual is taken. Then both the obtained iris image and the fingerprint image are separately as by the above procedures. The iris key is embedded in the fingerprint image to improve the template protection. So here we have to extract the iris key and fingerprint separately.

4. RESULTS

4.1 Dataset Description

In conjunction with the University of Bath, Smart Sensor Limited has collected a significant database of high quality iris images for use in research and evaluation. The pixel resolution of the collected iris image is 1280 x 960. Currently the full database consists of 800 people, i.e., 1600 eyes with 20 images of each left and right eye[23].

The hand vein database is a sample consists of images of 100 hands where each hand has 5 images, hence totaling to 500 images. This dataset is for both females and males in the range of 16-65 years age. Subjects are of healthy conditions and are from all folks of life including students, professors, engineers' workers, house wives, etc. [24].The CASIA fingerprint image database version 5.0(CASIA Fingerprint V5) contains 20,000 fingerprint image from 500 subjects. The fingerprint images in CASIA-fingerprint V5 were captured using a URU 4000 fingerprint sensor in a single session. A set of 500 fingerprint images for 100 fingers are used to evaluate of the proposed method.

4.2 Experimental Results

4.2.1 Existing method

The result obtained at various stage of our method is shown below.

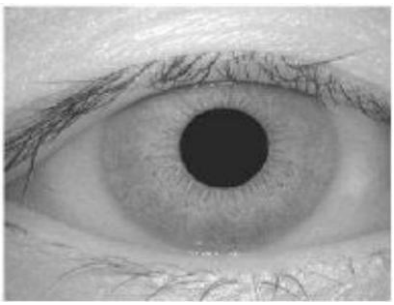

Fig. 4(a). Original Iris Image

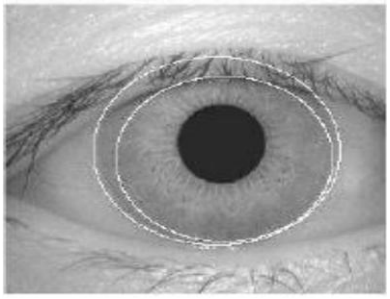

Fig. 4(b). Iris Image with Boundaries

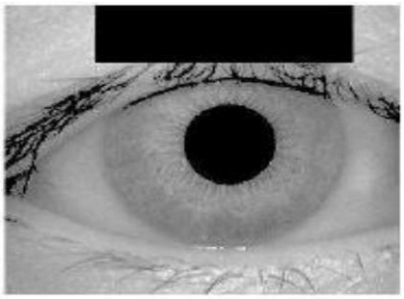

Fig. 4(c). Segmented Iris image

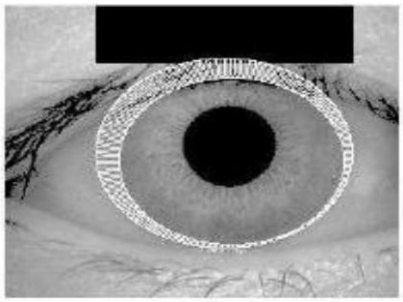

Fig. 4(d).Segmented Iris image with Boundaries

Fig.4(e). Polar array obtained after Normalization

Fig. 5(a). Original hand vein Image

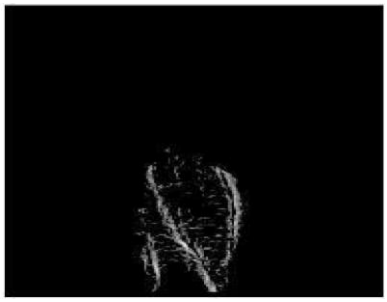

Fig. 5(b). Extracted vein image

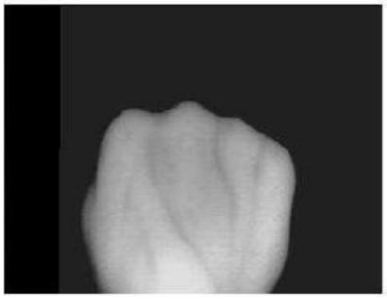

Fig. 5(c). Watermarked hand vein image

4.2.2 Proposed method

The result obtained at various stage of our method is shown below

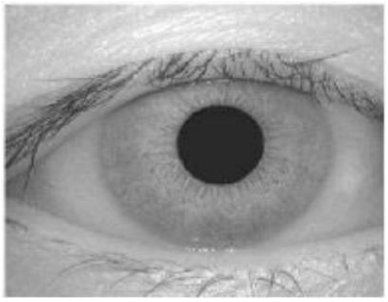

Fig. 6(a). Original Iris Image

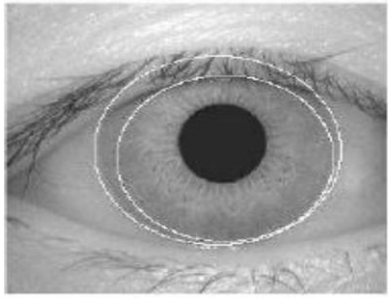

Fig. 6(b). Iris Image with Boundaries

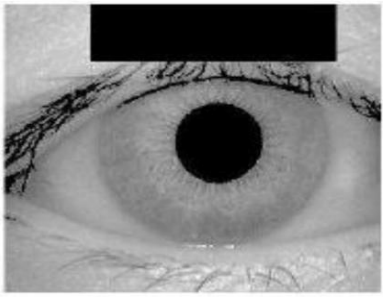

Fig. 6(c). Segmented Iris image

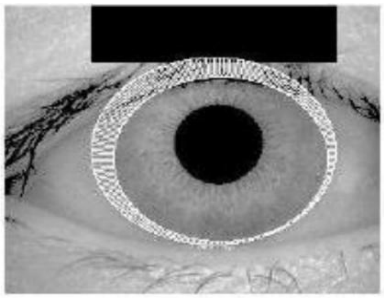

Fig. 6(d).Segmented Iris image with Boundaries

Fig. 6(e). Polar array obtained after Normalization

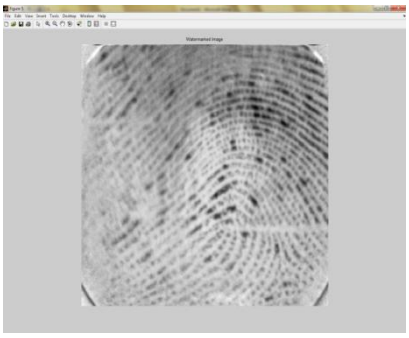

Fig.7(a). Watermarking fingerprint

Fig.7(b). Extracted watermark Fingerprint

5. CONCLUSION

In this paper we proposed authentication scheme to protect the ownership of digital images using a bimodal biometric watermarking approach. Presented methodology is based on efficient biometric recognition system for template protection. We have used a watermarking technology to improve the template protection based on the two modalities the iris and the hand vein. The iris template was extracted from the pre-processed iris image. Then the features of the hand vein were extracted. After this the extracted iris template was embedded in to the hand vein and stored in the database. Subsequently in recognition phase the iris template and hand vein features were extracted from the watermarked image. Fingerprint features are real human physiological characteristics, unique, permanent and not changeable. However, biometric characteristics are not secret and fake fingerprint image can be reconstructed easily. Therefore, fingerprint sample cannot be trusted for unattended-based authentication applications. The proposed method can be further improving the Accuracy by considering the embedding the iris data to fingerprint images using watermarking technology for template protection. The results obtained from the experimentation shows that our proposed watermarking techniques provide better results with higher accuracy. Furthermore, using two independent biometric watermarks and fusing information from them, makes users authentication more robust to poor quality images and attacks influence.

REFERENCES

[1] R. Yadav, Kamaldeep, R. Saini, and R. Nandal, "Biometric Template security using Invisible Watermarking With Minimum Degradation in Quality of Template," International Journal on Computer Science and Engineering, vol. 3, no. 12, 2011.

[2] J.L. Jimenez, R.S. Reillo and B.F. Saavedra, "Iris Biometrics for Embedded Systems," IEEE Transactions on Very Large Scale Integration (VLSI) systems, vol. 19, no. 2,2011.

[3] P.S. Revenkar, A Anjum and W.Z. Gandhare, "Secure Iris Authentication Using Visual Cryptography," International Journal of Computer Science and Information Security, vol. 7, no.3, 2010.

[4] AK. Jain, A Ross, and U. Uludag, "Biometric Template Security Challenges and Solutions," In Proceedings of European Signal Processing Conference, 2005.

[5] N. Hajare, A Borage, N. Kamble, and S. Shinde, "Biometric Template Security Using Visual Cryptography," Journal of Engineering Research and Applications (IJERA), vol. 3, no. 2, pp. 1320-1323,2013.

[6] C.L. Li, Y.H. Wang, and B. Ma, "Protecting Biometric Templates using LBP-based Authentication Watermarking," Chinese Conference on Pattern Recognition, pp. I -5,2009.

[7] Salil Prabhakar, Sharath Pankanti, and Anil K Jain. Biometric recognition: Security and privacy concerns. IEEE Security&Privacy, 1(2):33-42, 2003.

[8] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino. Impact of artificial gummy fingers on fingerprint systems. In ElectronicImaging2002, pages 275-289.InternationalSocietyforOpticsand Photonics, 2002.

[9] P. Poongodi, and P. Betty, "A Study on Biometric Template Protection Techniques," International Journal of Engineering Trends and Technology (IJETT), vol. 7, no. 4, 2014.

[10] K. Seetharaman, and R. Ragupathy, "Iris Recognition based Image Authentication," International Journal of Computer Applications, vol. 44, no. 7,2012.

[11] http://www.smartsensors.co.uk/irisweb/

[12] AM. Badawi, "Hand Vein database," At systems and biomedical engineering, Cairo University.

[13] Patrick J Flynn. Biometrics databases. In Hand book of Biometrics, pages 529-548. Springer, 2008./http://www.CASIA V5.com.