RESEARCH REVIEW JOURNALS
Volume-04
Issue-02
February-2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[UGC Listed Journal]

A Frame Work for Biometric Recognition Using Iris Data in Hand Vein Images

Smt. M Tirupathamma

Assistant Professor, ECE, JNTUH College of Engineering Jagitial

ARTICLE DETAILS

Article History
Published Online: 20February 2019

Keywords
watermarking; feature extraction; verification; extraction; implementation

ABSTRACT

Biometric acknowledgment is imperative technique for acknowledgment of individual as of late. Biometric security, which is the safety issue resulting from capability and violations of the layout details, is a frequent problem here. So as to deal with this issue, looks into have suggested various calculations to be stood up to by biometric mechanisms' protection. In this research, we use a watermarking innovation for improving the format security in biometric verification. Two methodologies, such as the iris and hand vein, are used to preserve the properties of vividness and constancy, as shown by. The following developments are used in our suggested plan for incorporating iris details into hand vein pictures using watermarking invention to boost format assurance in biometric recognition: 1) pre-preparing of iris and hand vein pictures, 2) Iris structure extraction, 3) Vein extraction, 4) Iris example implanting of vein pictures based on district of interest, 5) Storing mounted pictures. The iris illustration is derived from the mounted image during the acknowledgment point, and then the coordination is completed with query pictures. The item rule-based score level composition specifies the final validity inference. The implementation is performed in MATLAB, and the method's show is analyzed with FRR, FAR, and accuracy.

1. Introduction

Excessive use in electronic transactions, as well as the negative effects of extremism, have intensified the use of human authentication. To satisfy the need, people are now turning to biometric principles[1].

A pattern recognition system uses a person's distinctive physical features to recognize and validate him or her[2]. Recognition and verification are two main classes of activities that apply to a biometric method[3]. Various characteristics are taken into account in biometric methods, including face features, hand veins, way of walking, keystrokes, odor, ear, fingerprint, face, hand geometry, retina, palm print, iris, accent, and sign[4]. When paired with conventional validation systems, biometrics shows promise as a valuable method for ensuring legitimacy[5].

One of the most deep problems with biometric systems and information is their vulnerability to privacy concerns and adversarial attacks. As a result, rather than using basic documents, full proof techniques for storing biometric models must be used[6]. In biometric systems, approaches based on template use worldwide computing to remove characteristics after resizing a sub-image from the initial tactile image[7]. Using a function extraction system or mainly credited algorithms, a biometric prototype can be generated[8]. Using watermarking methods, such biometric models could be stored safely and efficiently secured[7]. Biometric watermarking appends biometric information in electronic product, allowing a person to communicate with online technology[9]. While using an embedding algorithm which is key based and a faux pattern, virtual watermarks can be primarily incorporated into the original information as a modified digital signal, greatly enhancing protection[10]. Watermarking is the practice of adding critical facts that people are unable to remember. If the template is hidden behind other biometric representations, it will guarantee multi - modal user verification[11]. By inserting confidential knowledge in the source code, it can be used to secure intellectual property rights[12]. Nevertheless, it is supposed to be resistant to certain biometric device threats[13]. The least significant bit (LSB) technique, in which the least significant bits of pixels are substituted for data encrypting, is the most commonly used watermarking technique[10].

Nevertheless, he growing need for authentication has necessitated work into creating irreversible, irreproducible biometrics. Human iris is another of these biometrics. Visual characteristics like circles, furrows, feckless and corona are used in iris detection. [14]. Iris identification has proven to be difficult because of the higher degree of random events in certain functions. Better precision could be obtained by incorporating additional human characteristics, particularly poking veins and hand backs, that are richer in veins than fingertips, according to new advancements in infrared method. As a result, hand vein identification is among the remote fields of biometric security science[15].

Hand vein patterns are observed to be unique among people and to continue for years in a person's life[16]. This vascular patterns are intricate, necessitating the creation of multiple sets of characteristics to guarantee adequate personal recognition[17, 11]. From the literature survey, [3], [4], [18], [19], [20], [21], [10] and [22], The developers talked about different template authentication protocols and how important they are for biometric template safety. In addition, we discovered which a reliable biometric identification methodology is needed for template security. The following are the article's key contributions :

I) To ensure the protection of biometric security models, we suggest a safe watermarking system.
II) During the recognition process, the implanted iris prototype is retrieved and matched using the algorithm that is suggested. The following is the

layout of the article's reaffirmation: The suggested technique for implanting iris data with hand vein pictures is presented in second section. The study findings are discussed in third section, and the article is concluded in forth section.

2. Suggested watermarking technology on inserting iris data to HND vein images

The objective of the biometric recognition method is to enhance template security by using watermarking methodology to insert iris data into hand vein photographs. The following measures make up the planned methodology for implanting iris data into hand vein photographs utilizing watermarking method, i) Pictures of the iris and hand veins were preprocessed, ii) iris template extraction, iii) Vein extraction, iv) Iris patter is embedded in vein photographs depending on the area of importance, v) Storing embedded images.

(i) Irish Image Pre-processing and key generation

Pre-processing is the first phase of our suggested approach, in which iris images are obtained and processed to obtain the iris key. The detail relevant to the iris component is extracted from the whole frame by corresponding translation.

a) Iris Localization

Nonetheless, optimization is considered efficient when the amount of pixels missing within the circular perimeter is kept minimized. Since the pixel values within the circular perimeter is reduced, calculation is quick and simple. The differential image's spikes can then be localized using non-maximum repression. Using a surface overlaps across two of its eight neighborhood associated pixels, the mechanism of non-maximum repression on a pixel with its differential imread(x, y) and direction theta(x, y) may be renowned. The pixel value of a point at (x,y) can be said to be maximal if it is not less than the pixels obtained from the two points of intersection. The poor edges that are under a particular target value and are not associated with an edge which is above the strong case by a chain of pixels being above the low threshold are then removed using amplitude threshold method. To execute the feature extraction method, the iris and pupil parameters are defined. The integro-differential regulator introduced by Daugman can be used to evaluate these parameters and radii. It's written as a formula(1) as

$$\max(r, a0, b0)\left|G_\sigma(r) * \frac{\partial}{\partial r}\oint r, a0, b0\frac{I(a,b)}{2\pi r}ds\right| \quad (1)$$

As a result, the above user scans the gradient image together with the boundaries of circles with large radii, acting as a circular detection algorithm. The maximum number, which can be estimated depending on the probability of all circles, can be used to measure the centers and radii of the circles. Hough transition is synonymous with a few problems. They are predefined threshold calculation by trial and error and calculation expansion. For each quest point and radius, eight-way synchronous points in the circle can be used to address these problems. Since eyelashes are not included in the iris key, the threshold definition may be used to separate them, and these pixels are labelled as noisy pixels.

b) Image Normalization

Normalization is the next step after iris segmentation in order to obtain an iris key and compare them. Unpacking the iris and converting it to polar counterpart are the two stages in the normalization procedure. Daugman's rubber layer system may be used for this. The coordinate system is fixed to the pixel's middle, and the points are translated to polar scale utilizing a rebinding algorithm. The following equation shows the updated variant of the system(2) as follows.

$$R = \sqrt{\propto \beta} \pm \sqrt{\propto \beta^2} - \alpha - R_1^2 \quad (2)$$

The iris radius is defined by R_1.

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

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

The picture's circular and angular resolutions are set to 100 and 2400, respectively. In the polar scale, each iris pixel's equal location is calculated. To deinterlace the normalized image to the actual image's dimension, the "interp2" feature is used. By splitting NaN, that is produced by the sections in the normalized image, by the number of the parts, a normalized value can be calculated.

c) Encoding

The method of removing the much more special attribute in the iris pattern is referred to as iris key generation. Just the phase data from the clatter is used since the given phase adjustments are not dependent on the image contrast. It is not utilized because amplitude data is based on not so appropriate variables. Phase details can be derived using 2D Gabor wavelets, in accordance to Daugman. It calculates that core area the corresponding phasor belongs to. The following equation can be used to do this(3).

$$H\{R_e, I_m\} = sgn\{R_e, I_m\}$$

$$\int p \int \emptyset I(\rho, \emptyset) e^{-\tan(\theta_0 - \emptyset)} e^{-(r_0-\rho)2/a^2} e^{-(\theta_0-\emptyset)^2/\beta^2} \rho d\rho d\emptyset \quad (3)$$

Based on its quadrant, H{Re, lm} has both a real and an imaginary component, with 1 or 0 as constituents. By segmenting a 2D normalized pattern into various ID wavelets and convolving them with ID Gabor wavelets, the Gabor filter could be utilized easily. Since Gabor filters fail to correctly reflect higher frequency elements, log-gabor filters are better than Gabor filters for representing normal. The LoG Gabor filter can be written as follows in equation (4) below :

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

The Gabor - convolve function generates an integrated value convolution output with a scale that is close to the original Image's size. By applying dual elements to any pixel of the image, the performance of Gabor-convolve can be used to create an iris key. Based on the positive or negative sign of the real and imaginary parts, each variable has a value of 1 or 0. When an element's mogul is very thin, it's called a noise bit, and it's incorporated with the noisy part produced from normalization.

(ii) Graphic pre-processing and feature extraction for hand veins

An collection of infrared light-emitting diode (LED) and a thermal camera are used to obtain photographs of the dorsal hand veins. In order to minimize noise, the collected hand vein image is first pre-processed.

Then, on the pre-processed hand vein image, add a mask. The picture generated after camouflaging is the same size as the input. Then, in the concealed picture you've developed, look for values more than zero. Kirsch's template extraction process is then used to remove the blood vessels from the hand vein illustration. It rotates a single concealed pixel of a hand vein image with a dimension of 3 x 3 in 45 degree installments through all 8 directions to evaluate the intensity of the edges. It is given by the equation (5) given below,

$$K_{a,b} = Max_{d=1\ldots8} \sum_{n=1}^{1} \sum_{m=1}^{1} W_{nm}^{(d)} . P_{a+n,b+m} \quad (5)$$

Here, d is the 8 direction as shown next,

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

Ultimately, the maximal magnitude in all directions for the chosen mask pixel of an image is calculated. The next step is to use a technique called local thresholding to distinguish the front and rear of the hand vein picture. It differs from traditional thresholding, which adjusts the threshold gradually as the images progress. The pixels of the hand vein image whose frequency components are well above a threshold are considered front values, while the rest of the pixels are considered rear values.

The technique's key concept is to calculate the mean m(x, y) and variance v(x, y) of the points in each pixel's rxr neighborhood. The differentiation is then carried out using the formula (6) as a guide given below,

$$T(x,y) = m(x,y) + cXv(x,y) \quad (6)$$

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

The vein domain is defined as the pixel value underneath the threshold. The local dynamic thresholding method's mean and variance was determined using the equations (7) and (8) below,

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

and

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

Our method's variance is determined using the updated equation (9) seen below,

$$v(x,y) = \sqrt{\frac{1}{r^2} \sum_{i=x-r/2}^{x+r/2} \sum_{j=y-r/2}^{y+r/2} (f(i,j) - m(x,y))^2} \quad (9)$$

The duration of the calculated value by Kirsch's process is determined here. It is then multiplied by the equation (10) given below.,

$$L = 0.97XLength\ of\ blood\ vessel\ obtained \quad (10)$$

Then set a threshold based on the pixel value you got. Ultimately, the characteristics of the hand vein are chosen as the pixel value underneath the threshold.

(iii) Embedding of iris pattern to band vein image

The steps for embedding an iris key into vein images are mentioned below.

The watermark image is the hand vein image H, and the source is the iris main image I(x, y) (x,y). The watermarked picture Hw is the result (x, y).

The various steps in watermark embedding is

I) The input watermark image H(x, y) is splitted into smaller parts of size B "B2, B3.....Bn of size MxN. The separated block is then ordered. The first wavelet coefficient with positive step and a value underneath the threshold T(x,y) is selected from the sorted block of the input image H(x, y).

II) Then one bit from the iris prototype J(x,y) is substituted for the second LSB of the chosen block of the watermark image H(x,y). In the equation below, this mechanism is represented(11),

$$C_W(x,y) = \begin{cases} LSB\big(C_x(x,y) - I(x,y) if phase\big(C_w(x,y)\big) \geq 0\big) \\ C_w(x,y) if phase\ \big(C_w(x,y)\big) < 0 \end{cases} \quad (11)$$

Where Cw(x, y) is the coefficient in block Bn' and T(x, y) is the threshold for whether or not to inject the watermark bit.

4)All bits of the iris template J(x,y) can be implanted if the number of bits in the iris template J(x,y) is less than the block size in the hand vein graphic.

5) To produce the final stable watermarked hand vein image, an IDWT (Inverse Discrete Wavelet Transform) is added to the watermarked hand vein coefficient after implanting all bits of the iris prototype J(x, y) in the hand vein image. The method of implanting a watermark is illustrated in the diagram below,

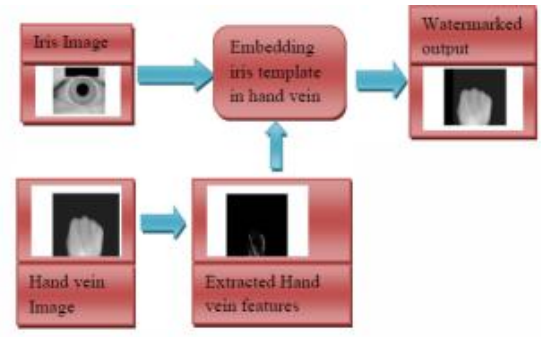

Fig.1. Watermark Embedding

(IV). Using Score Level Fusion in the Recognition Phase

There are two main phases in the identification process.

The first step is to remove the watermark.

The watermarked image is used as reference in this process, and the iris key and hand vein features are retrieved. There are several steps in the watermark extraction process.

The source is a watermarked image Hw(x,y) with the scale Hs(x,y) and the product is a restored watermark image Rw (x,y).

1) The watermarked image is grouped into blocks based on the information sub-band of the watermarked image. The watermarked image's blocks are 2M -1x 2N -1 in scale.

2) In every block, find the value below the T(x, y) threshold that has the initial coefficient of positive step.

3) If the inserted pixel value is higher than the average pixel value, pixel value 1 from the watermarked image is removed; else, pixel value '0' is extracted. This procedure is repeated until all of the pixels in the watermarked image are equal to y in equation (12).

$$H_s(x,y) = \begin{cases} 1, B_{(i)} > B_n, 0 < i < n \\ 0, \quad otherwise \end{cases} \qquad (12)$$

4) To achieve the watermark image H(x,y), a matrix equivalent to the length of the watermark image Hw(x,y) is generated and the retrieved pixels are put in it.

The iris and vein images of an object are taken during the identification process. The acquired iris image and hand vein image are then pre-processed independently using the steps described above. The iris key from the iris image and the vein characteristics from the vein image are acquired during this pre-processing phase. Even farther, we must equate the received function with the functionality stored in the database to determine if the source user is authentic or an imposter. However, to enhance template security, the iris key is inserted in the hand vein picture in the database. As a result, we must distinguish the iris key and vein picture.

Step 2: Matching

It is now possible to calculate the distance between the iris key produced from the input test image and the iris key retrieved from the embedded image stored in the database. Di is the distance between the input iris key and the retrieved iris key from the embedded image.

Similarly, the vein image attribute derived from the implanted image stored in the database is compared with the pre-processed vein image of the same individual. Ultimately, for the vein picture, a matching distance D: is calculated. Furthermore, using the sum law, the two normalized similarity distances Di is and DV ei are merged sequentially as seen in equation (13) below,

$$MS = \alpha * D_{iris} + \beta * D_{vain} \qquad (13)$$

Here, ∞ and β are two measured values that can be calculated with the help of a feature. A blend of linear and exponential functions is used in this article. If the cost of the matching score is less than the threshold, the weight is allocated linearly; otherwise, the score is calculated as exponential weight age. The matching score is determined by the value of MS. Individuals are eligible to join the scheme if their matching score is higher than the threshold value, otherwise they are disqualified.

3. Experiments & Results

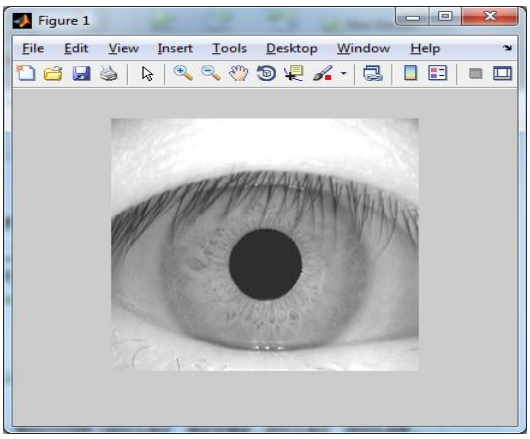

Fig.1. Input Iris Image

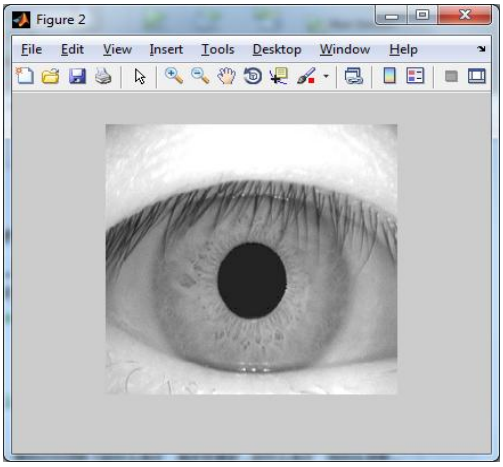

Fig.2. Input Iris Image in Double precision

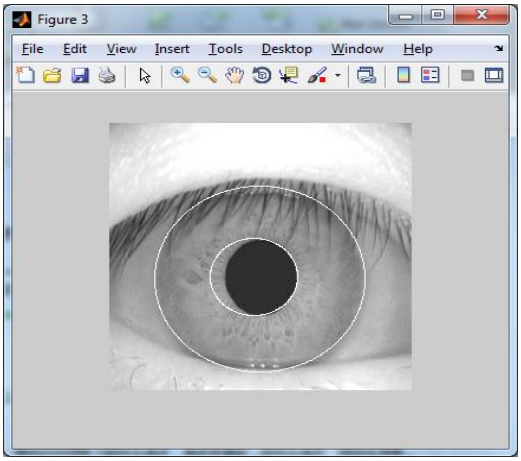

Fig.3. Iris Image after applying Thresholding

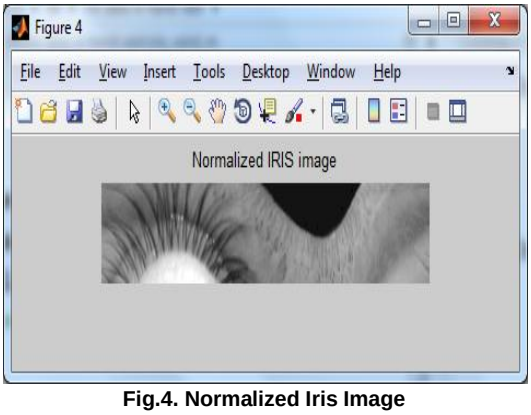

Fig.4. Normalized Iris Image

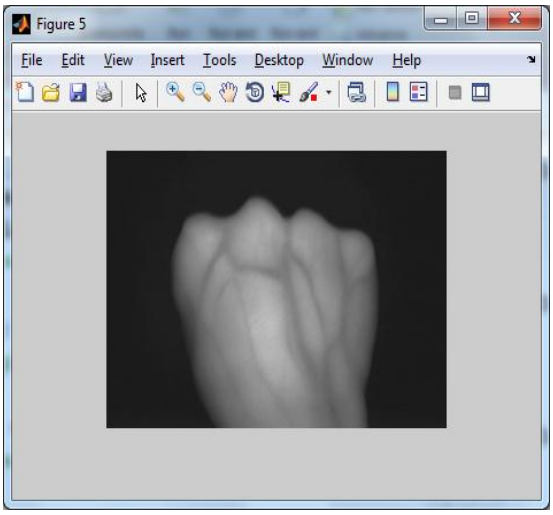

Fig.5. Input Hand Vein Image

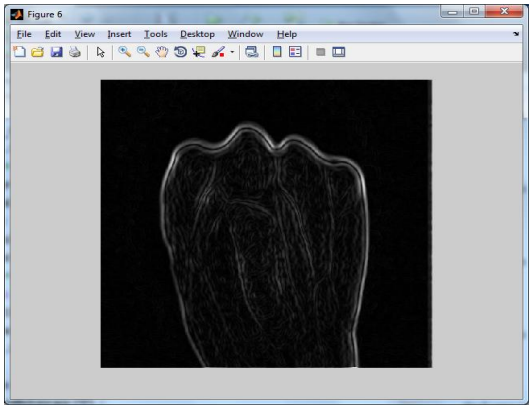

Fig.6. Image after Feature Extraction

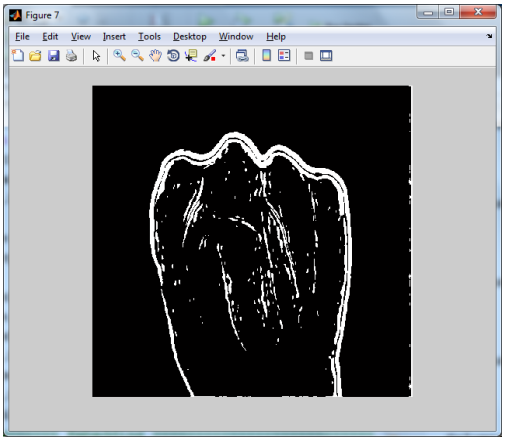

Fig.7. Image after converting Grayscale to Binary Image

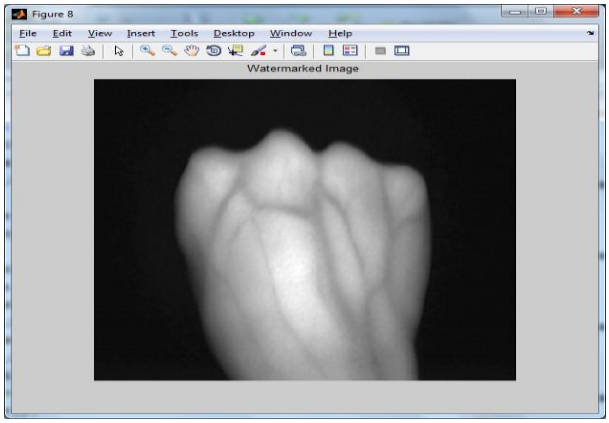

Fig.8. Watermarked Image

4. Conclusion

We, in this article, have introduced an effective biometric acknowledgment framework for layout insurance. Here, We utilized a watermarking technology to boost the format insurance based on both the iris and the hand vein mechanisms. The pre-handled iris image was separated from the iris layout. At that point the highlights of the hand vein were extricated. After this the separated iris format was inserted in to the hand vein and put away in the database. In this way in acknowledgment stage the iris format and hand vein highlights were separated from the watermarked picture. At long last the extricated highlights were coordinated with info question picture. A formal validation determination was taken based on the item rule-based score level mix. The results of the experiment show that our suggested watermarking techniques provide improved results with greater precision.

Different inquiry measurements will increase the precision of our proposed strategy by improving the installing efficiency and inserting field.

References

[1] 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.

[2] R. Yadav, Kama deep, 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. 12,20I I.

[3] 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.

[4] 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,noJ,20IO.

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

[6] 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.I320-1323,2013.

[7] 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.

[8] M. Arjunwadkar, and R.V. Kulkarni, "Robust Security Model for Biometric Template Protection using Chaos Phenomenon," International Journal of Computer Applications,vol. 3,no. 6,2010.

[9] D. Mathivadhani, and, and C. Meena,"Digital Watermarking and Information Hiding Using Wavelets, SLSB and Visual Cryptography Method," IEEE International Conference on Computational Intelligence and Computing Research (ICCIC),pp.I-4,2010.

[10] P.K. Sharma, and Rajni,"Analysis of image Watermarking Using Least Significant Bit Algorithm," International Journal of Information Sciences and Techniques (mST) vol. 2,no. 4,2012. [11] M. Fouad, A.E. Saddik, and E. Petriu, "Combining DWT and LSB Watermarking To Secure Revocable Iris Templates," 10th International Conference on Information Sciences Signal Processing and their Applications (ISSPA),pp. 25 - 28,2010.

[12] E. Mostafa,M. Mansour, and H. Saad,"Parallel-Bit Stream for Securing Iris Recognition," IJCSI International Journal of Computer Science Issues,vol. 9,no. 2,2012.

[13] S. Edward, S. Sumathi, and R. Ranihemamalini, "Person authentication Using Multimodal Biometrics with Watermarking," International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN),pp. 100 - 104,2011.
[14] K. Seetharaman, and R. Ragupathy, "Iris Recognition based Image Authentication," International Journal of Computer Applications, vol. 44,no. 7,2012.
[15] M.Y. Sheng, Y. Zhao, F.Q. Liu, Q.D. Hu, D.W. Zhang, and S.L. Zhuang, "Acquisition and Pre-processing of Hand Vein Image," pp. 5727 - 5729,20II.
[16] M.M. Pal, and R.W. Jasutkar, " Implementation of Hand Vein Structure Authentication Based System," International Conference on Communication Systems and Network Technologies, pp. 114 - IIS, 2012.
[I7] Sanchit, M. Ramalho, P.L. Correia, and L.D. Soares, "Biometric Identification through Palm and Dorsal Hand Vein Patterns," International Conference on Computer as a Tool,pp.I-4,20II.
[18] R.M. Thanki, and K.R. Boris agar, "Novel Approach For Multimodal Biometric System Using Compressive Sensing Theory Based Watermarking," International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR),vol. 3,no. 4,pp. SI- 90,2013.
[19] A Bamatraf R. Ibrahim, and M.N. Salleh, "A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit," Journal of Computing,vol. 3,no. 4,2011.
[20] S. Majumder, KJ. Devi, and S.K. Sarker, "Singular value decomposition and wavelet-based iris biometric watermarking," lET Biometric,vol. 2,no. 1,pp. 21-27,2013.
[21] G. Kaur, and K. Kaur, "Image Watermarking Using LSB (Least Significant Bit)," International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, no. 4, 2013.
[22] S. Malhotra, and C. Kant, "A Novel approach for securing biometric template," International Journal of Advanced Research in Computer Science and Software Engineering,Vol. 3,no. 5,2013.
[23] http://www.smartsensors.co.uk/irisweb/
[24] AM. Bandai, "Hand Vein database," At systems and biomedical engineering, Cairo University.

