ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
www.ijptonline.com
Research Article

A TWO-FOLD SECURITY APPROACH FOR AN IRIS TEMPLATE

Diksha Grover*[1], Krishna Devi[2], Preeti Gupta[3]
[1,2,3]Electronics and Communication Engineering Dept.
UIET, PU, Chandigarh
Email: d.grover1092@gmail.com

Received on 09-08-2016 *Accepted on 05-09-2016*

Abstract

Among different biometric recognition methods, iris recognition is considered as one of the most reliable, distinct, consistent, and stable choice. Template security is an important aspect of a biometric system. In this paper, a two-fold security approach based on run length encoding and steganography is proposed to protect the iris template. The proposed approach compresses the original template and the subsequent template is more secure when contrasted with the use of steganography alone. The execution of the proposed methodology is assessed and observed to be better in terms of Mean Square Error(MSE), Peak Signal to Noise Ratio (PSNR) value and histogram plot.

Keywords: Biometrics, template, run length encoding, steganography, data hiding, compression.

1. Introduction

A. Biometrics

Biometrics is assuming a noteworthy part in computerized individual identity frameworks conveyed to upgrade security everywhere throughout the world. Biometric recognition[1] or biometrics alludes to programmed recognition of people in light of their behavioral and/or physical qualities. Biometric recognition forms a link between a man and his identity on the grounds that biometric qualities can't be effortlessly shared, lost, or copied. In this manner, biometrics is by and large progressively being incorporated in different verification and security applications. A number of biometric traits such as fingerprint, iris and face are in use in various applications that deal with access control, checking for multiple enrollments (e.g. duplicate driver license), international border crossing and secure identification document (e.g. passport). Out of all the biometrics, iris is thought to be a reliable biometric for human identification for many reasons. Since the iris is an interior organ of the eye, it is shielded from outer wear and tear by the cornea, which is a highly

transparent film. Iris texture generation[2] is a chaotic procedure that happens amid the embryonic growth time frame. The benefit of the tumultuous structure of the iris is that even hereditarily indistinguishable monozygotic twins have distinct iris textures, despite the fact that their DNA fingerprint is the same. Long term stability of iris likewise makes it reliable for security applications. Additionally, the non-contact acquisition framework used makes it more hygienic and invulnerable to blunders. Front outlook of an eye is shown in Fig 1.

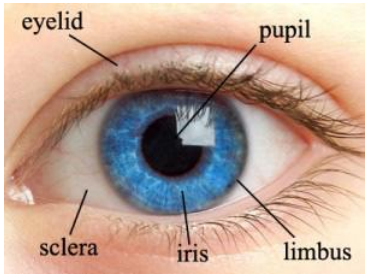


Fig 1. Front outlook of an eye.

B. Iris Recognition System

The earliest recognition using iris as a biometric trait was proposed and designed by John Daugman[2]. The goal of an iris recognition system[3] is to extract, represent and compare textural information present on the iris surface. A typical biometric system consists of acquisition, pre-processing, feature extraction, and matching modules as shown in Fig 2.

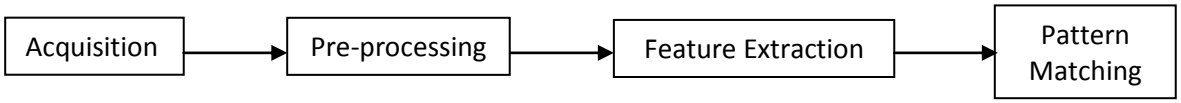


Fig 2. Block diagram of an Iris Recognition System.

a) Iris Acquisition: This deals with the picture capturing procedure of iris. Imaging is done in the visible/near infrared part of electromagnetic range.

b) Pre-processing: This step consists of segmentation/localization followed by normalization of the iris. Segmentation is done to isolate the iris section from the rest of the eye. Normalization is done to make the picture independent of the measurements of the input image so as to permit comparisons.

c) Feature Extraction: After iris is detected, various algorithms are used to encode the iris data. This process extracts features from the normalized iris images and encodes it to generate Iris Codes/Iris Signatures or templates.

d) Pattern Matching/Feature Comparison: After feature extraction, next step is to compare the code of the input Iris image with the code in the database.

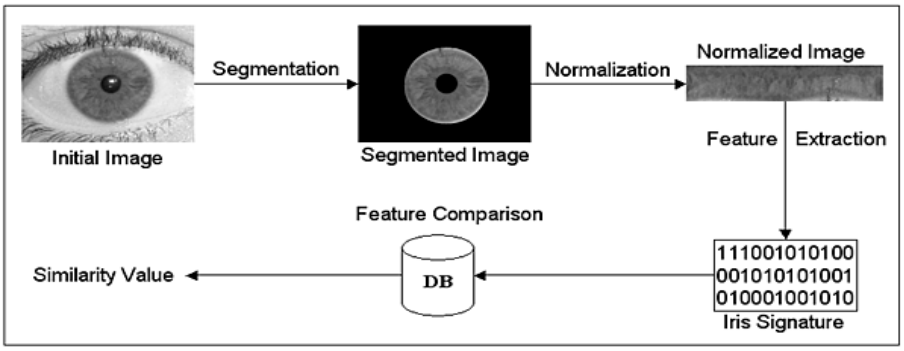


Fig 3. Steps involved in Iris Recognition process.

C. Template Security

During user enrollment the extracted feature set, labeled with the user's identity, is stored in the biometric system and is known as a 'Template'. Several factors that can affect the reliability of the template[4,5] are:

a) Accidental template corruption due to a system malfunction such as a hardware failure,

b) Purposeful modification of an enrolled template by an invader, and

c) Replacement of a valid template with a fake template for deterring system functionality.

Any manipulation with the stored templates in the database can lead to tampering with peoples' sensitive information or even illegitimate activities by anti-social elements. Thus template security is a significant area of study that needs consideration.

2. Related Work

A number of schemes have been proposed to protect the biometric templates from any fraudulent or accidental tampering. The earliest template protection scheme proposed was that of cancelable biometrics [6] whereby a compromised template is cancelled and replaced by another generated by updating the parameters of the applied transform. Another researcher proposed using a channel modulated cryptosystem for secure template storage[7]. Visual Cryptography scheme has also been proposed to secure the biometric template[8]. LSB Steganography was another template protection approach proposed to produce invisibility of the template by hiding it in a cover image[9].

3. Proposed System

A. Hypothesis

The most dangerous attack on a biometric system is against the template database. To sort out the problems related with database template security, an approach is presented for securing iris database templates. The approach proposes using an encoding theorem prior to the existing LSB Steganography approach for making the templates more secure.

B. Run Length Encoding

Run-length encoding (RLE) is a very simple form of data compression[10] in which runs of data (i.e., sequences in which the same data value occurs in many consecutive data elements) are stored as a single data value and count, rather than as the original run. For binary data(i.e. data consisting of only 0s and 1s) the data can be encoded as consisting of only the number of runs. For example, consider a data 000000111100000111. The RLE output of this data would be (6,4,5,3). Hence a data stream of 18 bits has been compressed to 4 bits. Thus this data encoding scheme compresses the data as well.

C. LSB Steganography

Steganography comes from ancient Greek words meaning 'concealed writing' and its goal is hiding the existence of message. It is feasible to apply steganography on any digital media like audio, video, images, network packets etc. The medium used to hide data is known as cover object or cover data and the result of steganography is stego object which contains secret information. In this approach, LSB steganography technique is used to hide Iris Code in cover image as shown in Fig 4.

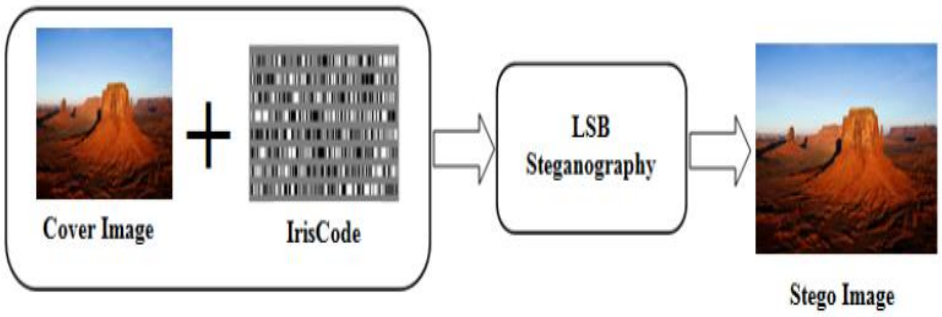


Fig 4. LSB Steganography Approach.

During enrollment process[9], the feature extraction module generates the Iris Code/template. LSB embedding module takes as input a cover image and the template. Using a random number generator, a random sequence of 6^{th}, 7^{th} and 8^{th} bit positions is generated. This sequence determines the bit positions of the cover image where you place the template bits. If the cover image is RGB, only the bit positions of one plane are substituted for. The cover image with the stored template bits is known as stego image, which is actually stored in the database instead of unsecured template.

For recovery of the template from the stego image, first the sequence of LSBs where Iris code is hidden is obtained, followed by extraction of bits from those positions. Then the template extracted can be matched with the template generated from the input of a query user.

D. Proposed System Architecture

a) Enrollment phase: During enrollment process, the proposed system architecture consists of the following two stages after the template generation as shown in Fig 5:

i. Template Encoding using RLE (Run Length Encoding)

ii. Hiding of the compressed template behind a cover image using steganography technique.

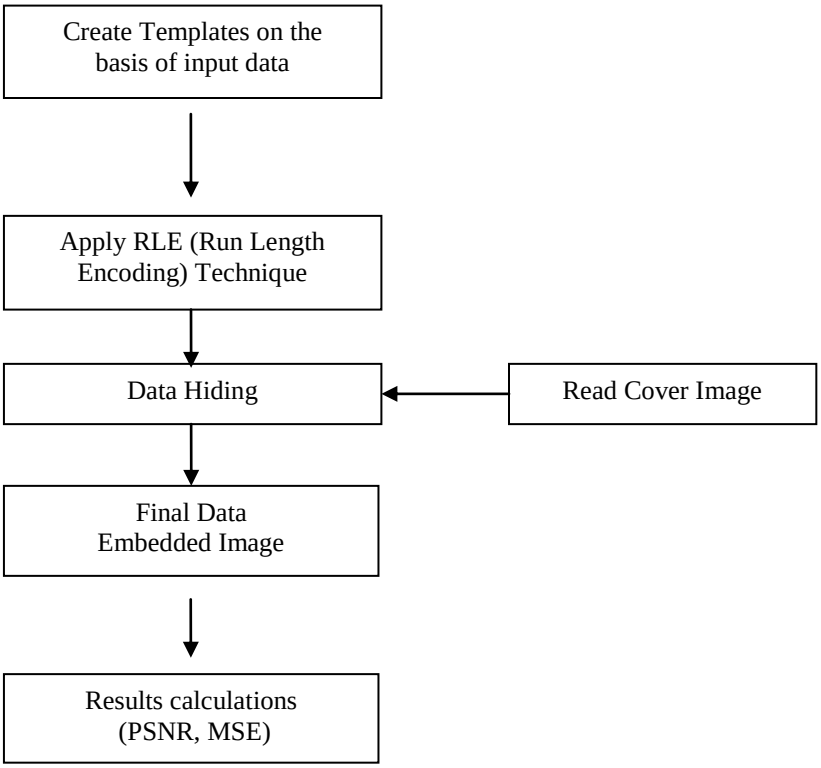


Fig 5. Architecture of proposed approach during Enrollment Phase.

b) Recognition phase: During recognition process, the following steps need to be performed to extract the template as shown in Fig 6:

i. Extract the hidden template from the cover image

ii. Decode the template to recover the actual Iris code

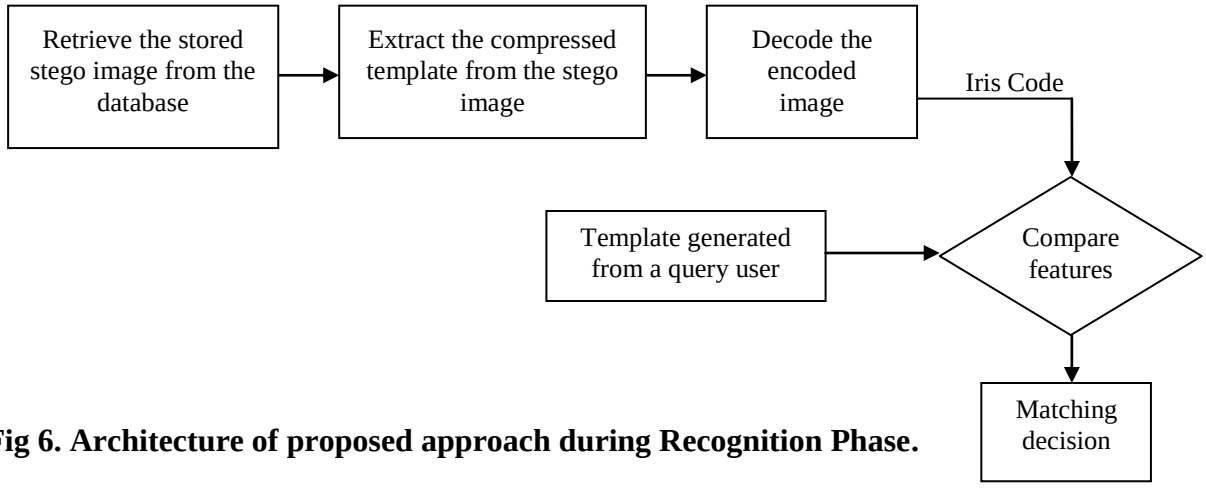


Fig 6. Architecture of proposed approach during Recognition Phase.

4. Experimental Results

The proposed system has been implemented on MATLAB using CASIA database consisting of 50 images. The following figures show the step-by-step implementation of the said approach.

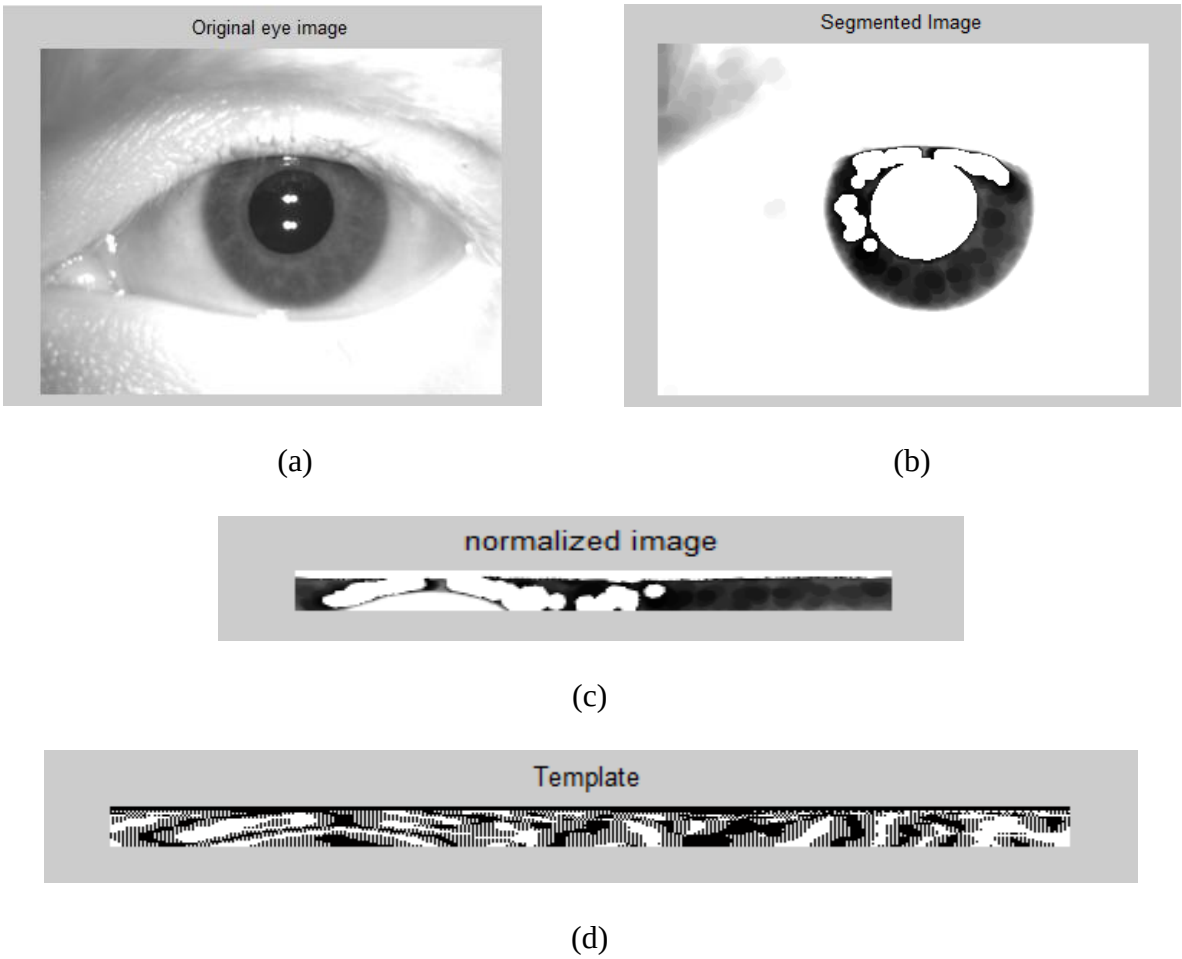


Fig 7. (a)Original eye image (b) Segmented iris image

(c)Normalized iris image (d) Generated Iris Code(template)

In this implementation, eye images have been segmented using Canny Edge detector and circular Hough transform[11] and normalized using Daugman's Rubber Sheet Model[2]. The template of size 20*480 has been generated by convolution of the normalized image with log-gabor[12] filter. It is this template that we wish to secure. In the proposed approach, run length encoding scheme is applied followed by hiding of the encoded template behind a cover image. Step-by-step implementation of the proposed approach has been shown in Fig 8 and Fig 9.

Since there is no visual difference between the cover and stego image, so Iris code is well protected behind the cover image. But if an attacker somehow detects the presence of the sensitive code hidden in the stego image and is able to retrieve it, the code he obtains is encoded RLE output which nowhere looks like a binary template. Hence the binary

template becomes undetectable even if it gets recovered from the stego image. Thus the proposed algorithm provides a two-fold security to the Iris template.

Fig 8. Encoded template.

(a) (b)

Fig 9. (a)Selected Cover Image (b) Obtained Stego Image.

5. Results and Discussions

The images of Iris are taken from CASIA-database. The cover image is 24-bit color image. To evaluate the performance of RLE scheme and LSB steganography applied to protect the iris template, CR, MSE and PSNR are calculated. The ROC curve plot is also used to analyze the effectiveness of proposed approach.

A. Compression Ratio

If we let n1 and n2 denote the number of information carrying units (usually bits) in the original and encoded images respectively, the compression that is achieved can be quantified numerically via the compression ratio(CR)[10]:

$$\mathrm{CR} = \frac{\mathrm{n1}}{\mathrm{n2}} \qquad (1)$$

This metric has been calculated after encoding the template since RLE also results in lossless compression of the data. CR for the proposed scheme for the complete database was calculated as 6.0685.

B. Mean Square Error

The MSE (Mean Square Error) between cover image X (s, t) and stego image X′ (s, t) is calculated using the equation (2), where m and n are the number of rows and columns of respective image. Lower the value of MSE, lower is the error. The equation for MSE[9] is given as:

$$MSE = \frac{\sum_{s=1}^{m}\sum_{t=1}^{n}[X(s,t)-X'(s,t)]^2}{m*n} \qquad (2)$$

MSE obtained after the application of steganography approach alone was found to be 0.0409, while for the proposed approach was obtained as 0.0276.

C. Peak Signal to Noise Ratio

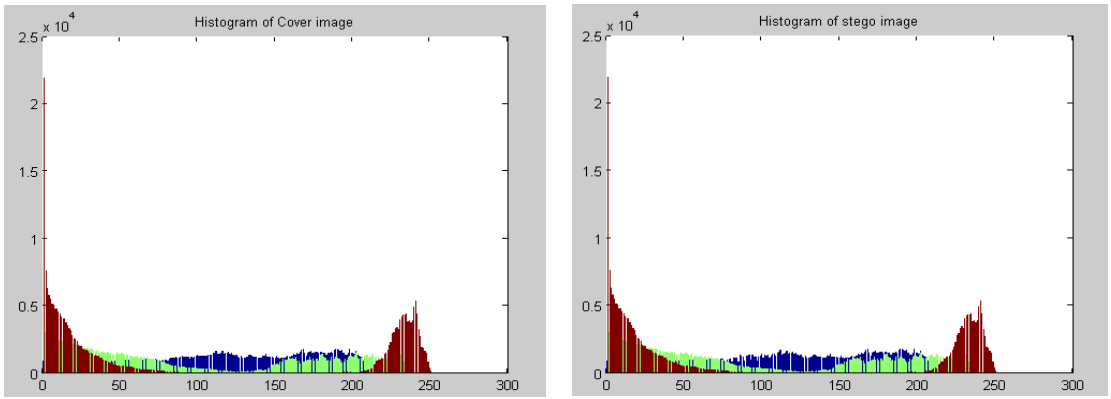
Difference between the cover image X (s, t) and the Stego image X′ (s, t) is measured via PSNR (Peak Signal to Noise Ratio). Greater the PSNR, more will be image quality and vice-versa. The PSNR is expressed in decibels(dB). For good perception, PSNR is expected to be more than 30 dB. It is calculated using the following equation[9]:

$$\text{PSNR} = \frac{10*\log_{10}(255*255)}{\text{MSE}} \qquad (3)$$

PSNR obtained after the application of steganography approach alone was found to be 62.0293 dB, while for the proposed approach was obtained as 63.7863 dB. PSNR of the images is acceptable value and shows that the image quality is preserved at good level.

D. Histograms

The histogram plot of cover image and stego image are described in Fig. 10 below. The histograms of both the images are found to be quite similar when compared.



(a) (b)

Fig 10. (a) Histogram of original cover image (b) Histogram of stego image.

E. Receiver Operating Characteristic curve

ROC (Receiver Operating Characteristic) curve is plotted for Genuine Accept Rate (GAR) against False Accept Rate (FAR) to analyze the performance of proposed scheme, by applying different threshold values as shown in Fig 11. False Acceptance Rate is the percentage of false pairs whose match score is higher or equivalent to the given threshold value. The Genuine Accept Rate is the portion of valid scores exceeding the threshold value. False Reject Rate is the percentage of true pairs whose match score is lower than the threshold value.

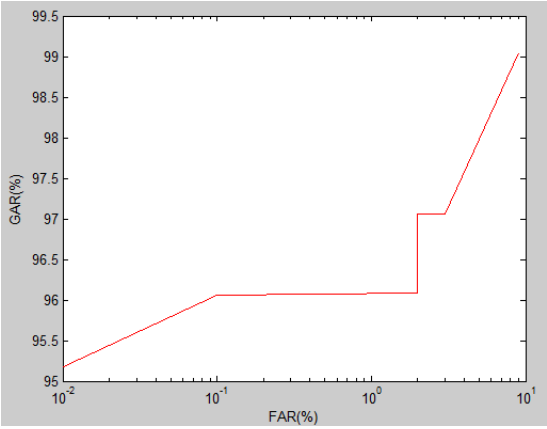


Fig 11. ROC curve obtained for the proposed approach.

6. Conclusion

As the biometric authentication systems are gaining more popularity, the security of database templates are becoming important. One of the shortcomings of biometrics is that once biometric data or template is stolen, it is stolen forever and can't be reissued, or disposed of. Thus, template security has become very critical in biometric recognition systems. In this paper, a hybrid method based on Run Length Encoding and Steganography has been proposed to protect the iris template. Experiments are carried out to examine the performance of the proposed approach. The resulting MSE and PSNR values are improved over the existing steganography technique and show that the image quality is preserved at a good level. ROC curve plot shows that the proposed approach provides a satisfactory performance. Thus, the proposed approach achieves a compression of the template as well as provides a two-fold security to the iris template.

References

1. A. Jain, A. Ross, and S. Prabhakar, “An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4-20, January 2004.

2. J. Daugman, "How Iris Recognition Works", *IEEE Transactions on Circuits and Systems for Video technology*, vol. 14, pp. 21-30, January 2004.
3. R.P.Wildes, "Iris Recognition: An Emerging Biometric Technology", *Proceedings of the IEEE*, vol. 85, no. 9, September 1997.
4. Anil K. Jain, Arun Ross, Umut Uludag, "Biometric Template Security: Challenges and Solutions", *13th European Signal Processing Conference*, Sept. 2005.
5. N. K. Ratha, J. H. Connell, R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", *IBM Systems Journal*, Vol. 40, Issue 3, 2001.
6. J. Zuo, N. Ratha, and J. Connell, "Cancelable iris biometric," in *Proc. Int. Conf. Pattern Recognition*, pp. 1–4, 2008.
7. E. Maiorana, P. Campisi, A. Neri, "Iris Template Protection using a Digital Modulation Paradigm", *International Conference on Acoustic, Speech and Signal Processing*, pp. 3759-3763, May 2014.
8. P.S.Revenkar, Anisa Anjum, W.Z. Gandhare, "Secure Iris Authentication Using Visual Cryptography", *International Journal of Computer Science and Information Security*, Vol. 7, No.3, 2010.
9. S. Chaudhary, R. Nath, "A New Template Protection Approach for Iris Recognition", *4th International Conference on Reliability, Infocom Technologies and Optimization*, September 2015.
10. M. Arif, R.S. Anand, "Run Length Encoding for Speech Data Compression", *International Conference on Computational Intelligence & Computing Research*, pp.224-227, December 2012.
11. S.Singh, S.Singh, "Iris Segmentation Along with Noise Detection using Hough Transform", *International Journal of Engineering and Technical Research (IJETR)* ISSN: 2321-0869, Vol. 3, Issue 5, May 2015.
12. A.T. Kahlil, F.E.M. Abu Chadi, "Generation of Iris Codes Using 1D Log-Gabor Filter", International Conference on Computer Engineering and Systems, pp.329-336, 2010.

Corresponding Author:

Diksha Grover*,

Email: *d.grover1092@gmail.com*