Volume 8, No. 5, May – June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Improving Iris Template Security using Genetic Algorithm

Neha Mahajan,
Research Scholar
Department of Electronics and Communication Engineering
DAVIET
Jalandhar, Punjab, India

Aarti Koccher
Assitant Professor
Department of Electronics and Communication Engineering
DAVIET
Jalandhar, Punjab, India

Abstract: Biometric recognition system is used to identify the person based on their behavioral characteristics. Different traits are used to authorize the identity of the person. Iris recognition is one of the biometric recognition systems which are highly in use nowadays. But the only issue that exists in this biometric trait is related to the security of the iris data which is maintained by the medical institutes to perform further research and for the further treatment of the patient. Lot of techniques and mechanisms had been developed in last few years which are capable to secure the iris template but are not able to provide the high level security. In this paper, we provide a new type of mechanism for high level security to the iris template by using the concept of data hiding. For the purpose of data hiding the concept of GA i.e. Genetic Algorithm is applied along with the encryption process with a valid key. We also provide a briefing to the stages that are followed while applying the proposed work. The simulation is performed under MATLAB. The comparison is done between the proposed work and LSB technique of data hiding. The performance evaluation parameters like Receiver Operating characteristic Curve (ROC), False Acceptance Ratio (BER), Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) are considered for the evaluation of the proficiency of the proposed work in contrast to the traditional Least Significant Bit (LSB) mechanism and it is achieved that the security level is high in the proposed work as compare to the previous.

Keywords: *Biometric Recognition, Iris Template protection, Genetic Algorithm.*

I. INTRODUCTION

Iris recognition is the method that is used for the identification purpose based on unique patterns that is ring shaped region surrounding the pupil of the eye. Iris recognition is the most advance and reliable fast access recognition technique used to achieve our task in limited period of time [1]. The iris has the fine texture because of which the identification is easier and reliable. Traditionally, the iris recognition was based on the direct matching of the feature [2]. In this method, a data set of the images was made from that data set the most appropriate image was selected.

The stage in the process of iris recognition is categorized as follows: [3]

a) Feature Extraction
b) Image Acquisition
c) Localization or Segmentation
d) Normalization

A. Feature Extraction: is a process of extracting the functions from an image. These features are used to specify quantifiable property of an object which can be classified as:

- **General features:** these types of features include color, shape and texture of the image [4]. Based on the abstraction level of these features it can be further classified as:
  - **(i) Pixel level features:** features are evaluated at each pixel in this type of features. Color is an example of this category.
  - **(ii) Local level features:** features are evaluated over the results of subdivision of the image band on edge or image detection.
  - **(iii) Global features:** these types of features are calculated over the entire image. Moreover, it can be performed on sub-area of an image.
- **Domain specific features:** in this category, application dependent features are laid. Consider an
- Example such as human faces, fingerprints and conceptual features [5]. Moreover, they are considered as low level features which are derived on the basis of requirements [6].

Consequently, all the features of an image can be classified into a category of low level and high level features [7]. Low level features can be extracted directly from an image whereas a high level feature is based on the low level features [8].

B. Image Acquisition

Image acquisition is a process of capturing an image by a camera and then performs conversion into a manageable entity. After the image acquisition has done, it processed further for future use. In such process, three steps are involved such as energy, an optical system and a sensor. Energy reflected from the object of interest, an optical system which spotlights the energy reflected on the object and a sensor that measures the amount of energy [9].

C. Image segmentation

Segmentation is the process of sectioning the digital image into number of regions which are called as pixels. The image obtain by the segmentation is more informative, clear and expressive that will easily depicts the information present in the pixel. The lines, boundaries, curves etc that are present in the image are detected by the image segmentation process. As the output of the image segmentation is the region that is segmented or is the set of the contour that are also taken from the image the pixels that are presented in the image are related

to each other on the behalf of some properties [10]. The properties can be color, intensity or texture. Image segmentation play an important role in the medical imaging, some of the uses of the image segmentation in medical imaging is described as below [11]:

- Tumors detection process
- It is used in measuring the tissue and their volumes
- Surgery done by using computer systems.
- Diagnosis
- Treatment plans
- Studying of abnormal structure

D. Image Normalization

Normalization is a process of changing the range of pixels intensity value. It comes in the category of image processing where normalization is a vital part [12]. Contrast stretching is another term used for normalization. One of the applications of normalization is to enhance the poor contrast of an acquired image due to glare. The main idea behind using this concept is to achieve consistency for a set of data signals and so as to avoid distraction.

II. TECHNIQUES USED

The techniques used for the proposed work to secure the iris template are as follows:

Gabor Filter

Gabor wavelet technique is used in image processing where it is separated into two series of one- dimensional ones. This technique is basically used to detect the edges, corners and blobs of the face image. Gabor functions helps to extract the features especially in texture-based image analysis. The two approaches i.e. edge detection that is done from the feature image and corner detection with the help of combination of responses to several filters with a different orientation [13].

GA (Genetic Algorithm)

GA stands for Genetic algorithm and this technique implements the optimization strategies. The parameters and operations used in this technique are as follows:

- Selection
- Crossover
- Mutation

Selection is a parameter which is used for selecting the various solutions which can be preserved or which can be able to reuse and which are not useful. The selection parameter aims to select the best solution and vanish or eliminate the worst solution which is not suitable. The good or best solution can be identified on the basis of fitness value. Fitness value is a parameter. Fitness function generates a value which is quantifies the solution optimally. Then on the basis of various fitness values corresponding to every solution best solution is selected. Following equation is used for assigning the fitness value:

- $$minimize\ f(d,h) = c\left(\frac{\pi d^2}{2}\right) + \pi dh \qquad (1)$$
- $$subject\ to\ g_1(d,h) \equiv \left(\frac{\pi d^2}{4}\right) \geq 300 \qquad (2)$$
- $$variable\ bounds\ d_{min} \leq d \leq d_{max} \qquad (3)$$
- $h_{min} \leq h \leq h_{max}$

III. PROBLEM FORMULATION

Iris recognition is most reliable and accurate biometric recognition process. On the basis of the iris recognition in this process the iris pattern of the human eye is captured then this captured image is converted into the frame using the image processing that will convert it into the coded digit that is called as iris code. One of the weaknesses of biometrics is that once a biometric data or template is stolen, it is stolen forever and cannot be reissued, or discarded. In the traditional method LSB technique was used. In such process iris template has been hidden under the cover image. As a result, security was enhanced because it becomes impossible for an imposter to find out which LSB holds the iris code bits without knowing random sequence of bits. But it is most common method for data hiding we need to update it. Therefore a new algorithm is needed to propose that will consider all these problems of iris recognition system.

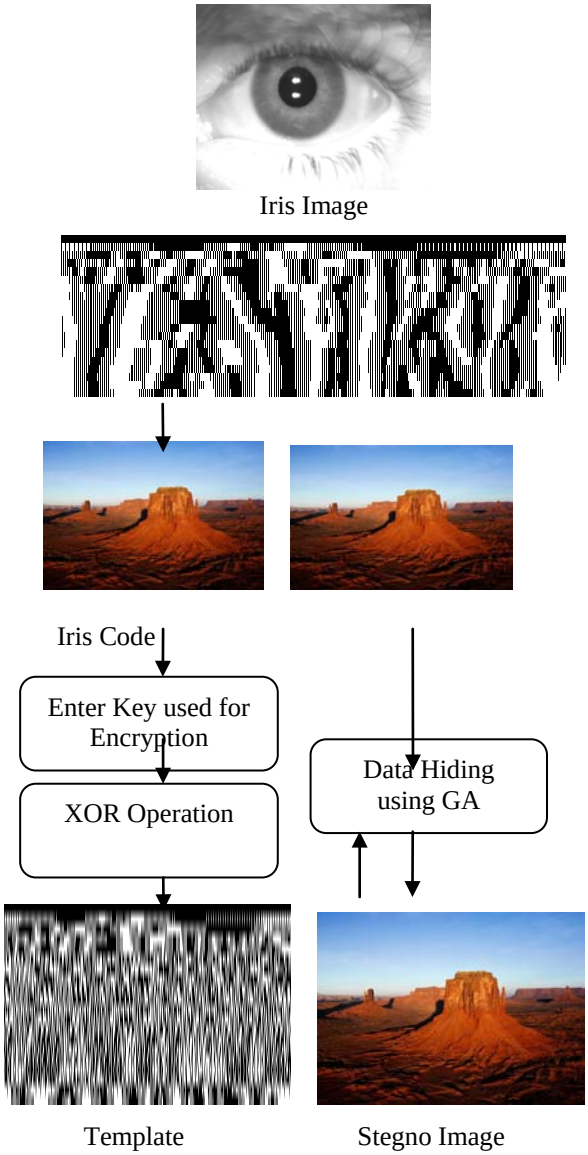

Figure1.Flow of the proposed work

IV. ALGORITHM

The algorithm for data hiding and data extraction of the present work are as follows:

A. Data Hiding: The first part of the proposed work is to hide the data of the database for the security purpose. In this process, the images of iris are hidden behind an image by generating some codes corresponding to every iris image. The technique that is used under this process is Genetic Algorithm which is used to hide the image.

1. First step is to input an image of iris from the image dataset.
2. Next step is to extract the features set from the iris image.
3. In this step a key is generated by using the extracted features of the image.
4. After this, next step is to apply the XOR operation on extracted feature sets and the binary key that were generated in previous step.
5. Then the genetic algorithm will be applied to the image for the purpose of hiding the data or image.
6. After hiding the data, the database will be created which is secured by applying the key or data hiding schemes.

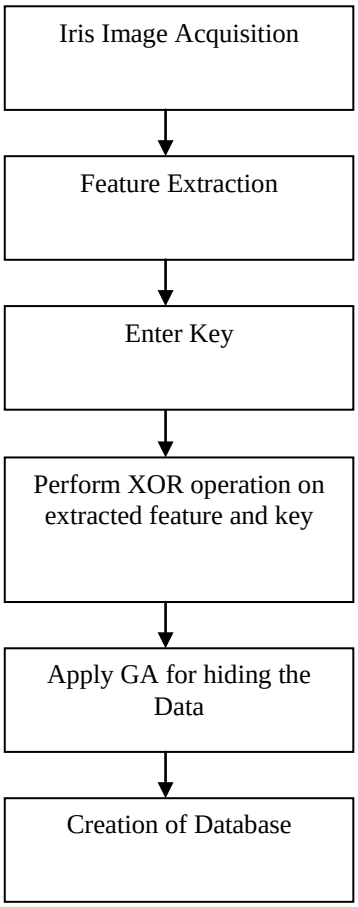

Figure2.Block Diagram of Data Hiding

***B. Data Extraction*:** After making the database secure by applying the data hiding techniques next step is to extract the hidden data in order to access the data. The algorithm for extracting the data is as follows:

1. Select an image from the database behind which the data or information is hidden.
2. To extract the features from the image as similar to the previous section of data hiding.
3. Enter the key which was generated in order to hide the data.
4. After this the matching of the extracted features and key will be done.
5. To evaluate the performance of the present work in the form of various performance Quality parameters such as
   (i) PSNR(Peak Signal to Noise Ratio):
   (ii) MSE (Mean Square Error),
   (iii) ROC (Receiver Operating characteristic Curve)
   (iv) FAR(False Acceptance Ratio)

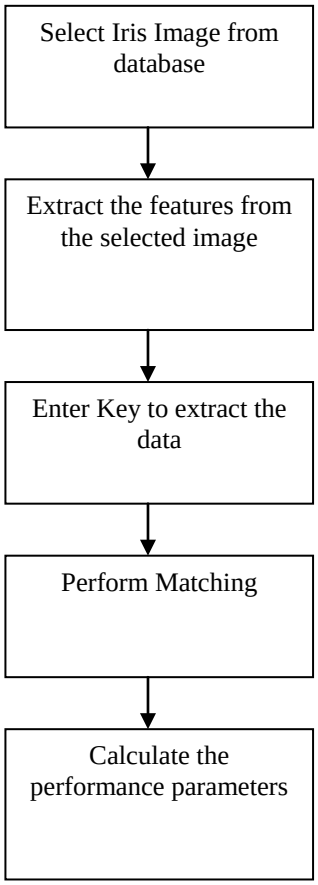

Figure3.Block Diagram of Data Extraction

V. RESULTS AND DISCUSSIONS

This segment of the work explains the results that are obtained after implementing the proposed work. The proposed work is comprises of the motive to maintain the security of the iris template to preserve the consistency and confidentiality of database. The proposed work implements the genetic algorithm to hide the iris template behind the cover image. For the purpose of simulation total 5 images are considered and the results are evaluated on the basis of these images.

The graph in figure 4 depicts the comparison between proposed work and LSB Approach on the basis of PSNR with respect to all of the images. From the graph below it is observed that the PSNR of proposed work is higher as

compare to the LSB Technique which proves the proficiency of the proposed work.

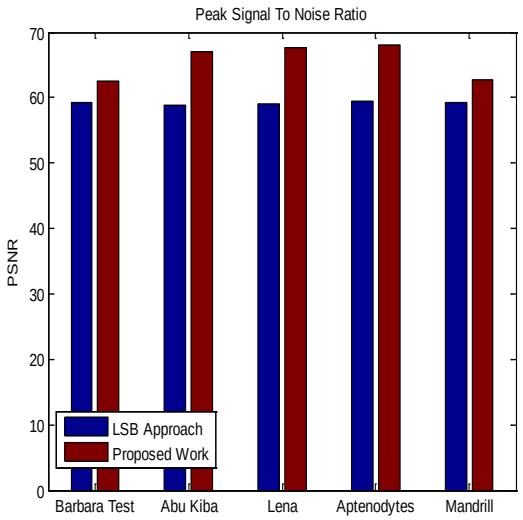

Figure 4.Comparison graph of PSNR

The graph in figure 5 depicts the comparison between proposed work and LSB Approach in the form of MSE with respect to all of the images. From the graph below it is observed that the MSE of proposed work is low as compare to the LSB Approach which proves the proficiency of the proposed work.

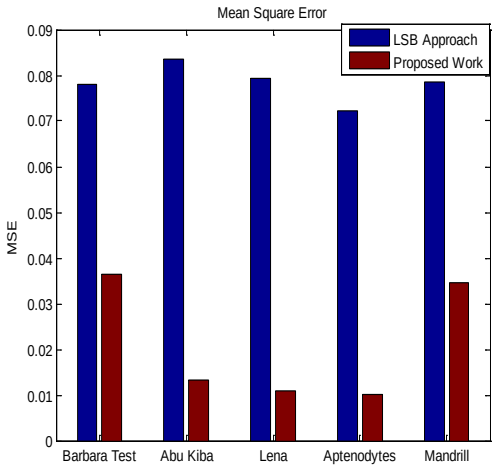

Figure 5. Comparison graph of MSE

The graph in figure 6 depicts the comparison between proposed and LSB Approach in the form of BER with respect to all of the images. From the graph below it is observed that the BER of proposed work is low as compare to the LSB Approach.

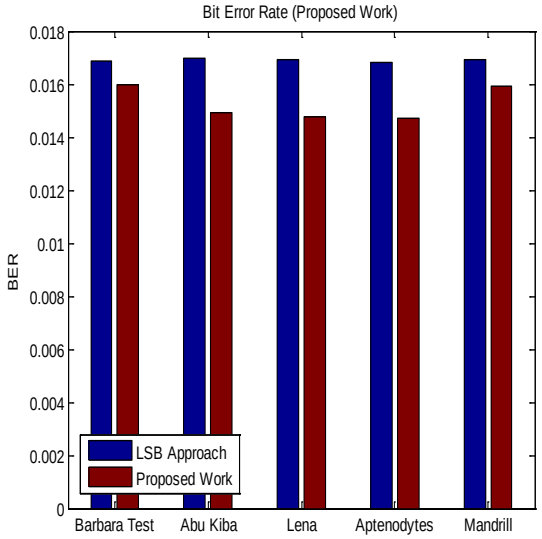

Figure 6.Comparison graph of BER

The graph in figure 7 depicts the comparison between proposed and LSB Approach on the basis of ROC curve. It defines the performance of the binary classifier system. The corresponding curve is plotted with the Genuine Acceptance Rate i.e. GAR against the False Accept Rate i.e. FAR at various threshold settings. From the graph below it is observed that the ROC of proposed work is high as compare to the LSB approach.

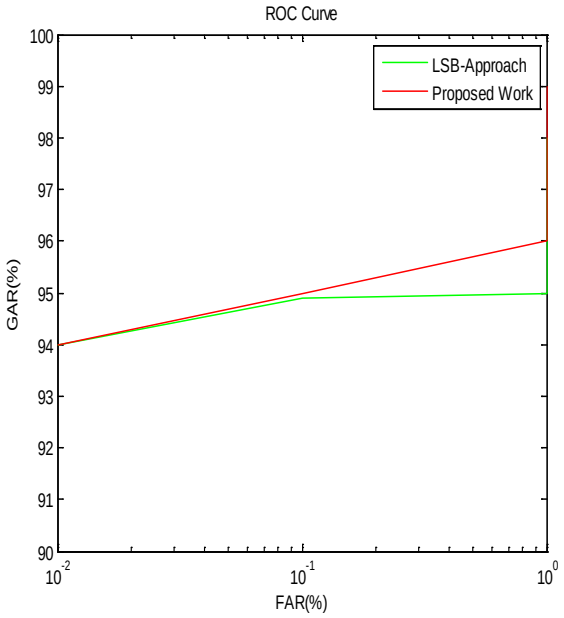

Figure7.Comparison of ROC curve

The following table1 depicts the comparison of proposed and LSB approach on the basis of five test images in the form of performance parameters i.e. Mean Square Error, Bit Error rate.

The work has better and efficient results as compare to the traditional and Peak Signal to Noise Ratio. From the table below it is concluded that the proposed LSB technique.

Table I. Parameter comparisons between proposed work and traditional work (LSB)

S. No	*Image Name*	*Technique*	*MSE*	*BER*	*PSNR*
1	Barbara Test	LSB	0.0779	0.0169	59.2129
		Proposed	0.0363	0.0160	62.5277
2	Abu Kiba	LSB	0.0834	0.0170	58.9169
		Proposed	0.0132	0.0149	66.9347
3	Lena	LSB	0.0792	0.0169	59.1427
		Proposed	0.0110	0.0148	67.7163
4	Aptenodytes	LSB	0.0722	0.0168	59.5476
		Proposed	0.0103	0.0147	68.0198
5	Mandrill	LSB	0.0767	0.0169	59.2842
		Proposed	0.0293	0.0158	63.4620

VI. CONCLUSION

Security has been become the main issue in the today's world. Various security and authentication methods or techniques are used to secure the iris template. We implement the concept of securing the iris template by using the genetic algorithm. The purpose of this work is to maintain the privacy and confidentiality of the biometric feature i.e. iris. The concept of image steganography and encryption is implemented to make the template secure. The results are evaluated by considering the five various test cover images and then the results of implemented work is compared with LSB approach and proposed technique leads to the most proficient results. The BER, MSE and PSNR are used to evaluate the performance of the implementation.

The table2 below defines the comparison between proposed work and LSB technique that was implemented in the traditional work. The table compares the LSB and present work in terms of Mean Square Error, Bit Error Rate, Peak Signal to Noise Ratio and Security. And it concludes that the proposed work is better than the previous work in every aspect such as the level of security is high whereas in LSB it was medium.

Table 2.Comparisons between proposed work and traditional work (LSB)

S. No.	Parameters	LSB (Traditional)	Proposed Work
1.	MSE	Medium	Low
2.	BER	High	Low
3.	PSNR	Low	High
4.	Security	Medium	High

VII. REFERENCES

[1] S.E. Baker, Empirical evidence for correct iris match score degradation with increased time-lapse between gallery and probe matches, SPRINGER, vol. 5558, pp. 1170–1179,2009.

[2] S.E. Baker.," Degradation of iris recognition performance due to non-cosmetic prescription contact lenses.", Computer vision and image understanding, Vol. 114, No. 9, Pp 1030–1044, June 2010.

[3] A. Czajka, "Influence of iris template ageing on recognition reliability", CCIS, Vol 452, Pp 284–299, November 2014.

[4] J. Daugman," New methods in iris recognition.", IEEE, Vol. 37, No. 5, Pp 1167–1175, October 2007.

[5] J. Doyle, K. Bowyer, "Robust detection of textured contact lenses in iris recognition using BSIF", IEEE Access 3, Pp. 1672–1683, August 2015.

[6] S.P. Fenker, "Experimental evidence of a template aging effect in iris biometrics" (2011).

[7] J. Galbally, "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms", ELSEVIER, Vol. 117, Pp. 1512–1525, 2013

[8] K. Hollingsworth, "Pupil dilation degrades iris biometric performance.", ELSEVIER, Vol. 113, No. 1, Pp150–157, January 2009.

[9] Jonas Nyasuslu, "Literature Study of Iris Biometric Recognition", IDA, Pp 1-5, 2008.

[10] SimranjeetKaur et al. "Survey of Different Approaches in Biometric Iris Recognition System", IJARCSSE, Vol 4, Issue 7, Pp 768-771, 2014.

[11] A. Malikarjuna. "Biometric Security Techniques For Iris Recognition System", IJRCTT, Vol 2, Issue 8, 2013

[12] UpasanaTiwari et al. "Study of Different Iris Recognition Methods", IJCTEE, Vol 2, Issue 1, Pp 76-81, 2012

[13] Donald M. Monro . "DCT based Iris Recognition", IEEE, Vol 29, Issue 4, 2007