A New Enhanced Template Protection Algorithm on Iris Recognition

Monis Khan, Suraj Yadav

Abstract*: Over the past few years, biometric systems have become prominent in terms of verification of the user identity due to increased demand of security in the networked society. Iris recognition system is a novel technology for the verification of user which is considered as the most secure, reliable and stable technique. It is generally accepted in the areas with high security. Though, security is major concern in this field, a significant number of approaches have been proposed to secure iris biometrics, But still, there is a scope to improve these techniques. Thus, in this work, a novel model is proposed which employs a bitmask compression technique to secure the template obtained for iris by compressing its actual size. In addition; SVM is used for the classification process. Mean Square Error, Bit Error Rate, PSNR, and GAR are different parameters which are used for measuring the effectiveness of the proposed model. The simulation results are carried out in MATLAB software and the comparative results validated the efficacy of the novel model with respect to security, efficacy and accuracy.

Keywords: Iris recognition, Bitmask compression technique, Support Vector Machines (SVMs) technique.

I. INTRODUCTION

There are various biometric recognition techniques, among which iris recognition is considered as the most reliable, distinctive, secure and steady technique.

The pattern recognition approaches which are based on distortion-free and high-resolution images of human eyes' iris are used by the Biometric iris recognition.

In the human body, the iris is that organ, structure of which remains constant throughout all life. Therefore, it acts as an optimal biometric for ascertaining the person's identity.

At the present time, iris recognition is the most reliable technique of validating the individual's identity as it consists of very less amount of error and is a quick approach.

In this system, the individual's eye's retina's high-resolution images are taken and after that pattern recognition is used in order to read and match the person's iris patterns with the patterns which are stored in the database of biometric [1].

The diagram given below represents the various steps involved in iris recognition system:

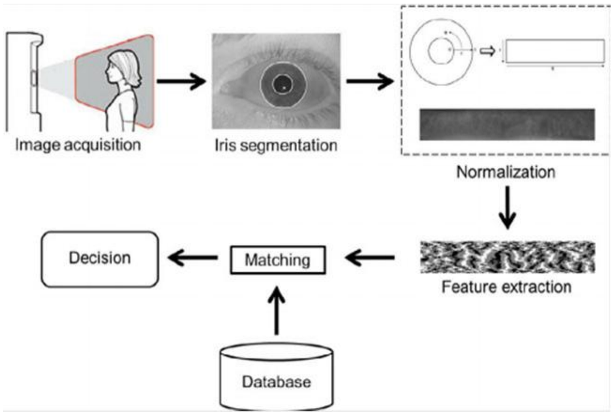

Fig. 1. A block diagram of an iris recognition system

A. Iris recognition process

Iris recognition process comprises of 3 different steps which are delineated below:

- Image capture: In the initial step, the iris's image of the individual, whose identity is required to be confirmed, is captured. The image can be captured manually or automatically, however, it must be assured that iris should be in proper focus and the image must be captured very clearly
- Locating the iris and optimizing the image: In the next step, the system initially optimizes the image's clarity and focus. After that, it finds the boundaries of the iris and subsequently pupil's center that is also the circular iris's center. At last, it scrutinizes the iris image's area that is appropriate for the extraction of features and scrutiny. When the area that is appropriate for extraction of feature is identified, then the optimization of the region of the iris is done by eradicating deep shadows, areas covered through eyelids and reflective regions. Also, the area which is optimized is normalized in the rectangular block in order that it consists of constant dimensions that are analogous with another iris scan. It must be noted down that it is impossible to contrast the optimized image of an iris with the iris image which is stored in the database. Instead of this, the biometric templates are stored in the database of biometric that comprise of iris' encoded structure characteristics that are hauled out from image after implementing Daugman's rubber sheet model.

Manuscript received on February 15, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author

Monis Khan*, Department of Computer Science and Engineering, Jagannath University, Jaipur, India. Email: khan.monis6@gmail.com

Suraj Yadav, Department of Computer Science and Engineering, Jagannath University, Jaipur, India. Email: suraj@jagannathuniversity.org

- Biometric template storage and/or matching: In the last step, the biometric templates or encoded structural attributes are stored in the database of biometric while doing individual's enrollment.

When the iris scan is considered for the verification purpose, then the scanned image's biometric template gets a match with the biometric templates which are stored in the database.

B. Superiority of iris

There are numerous features of iris due to which the biometric system has become extremely trustworthy and robust to be utilized in identity management solutions in contrast to other biometric features:

- Irises are distinct even for alike twins.
- An iris has more than 266 degrees of freedom (i.e. the structure variable's number that can change simultaneously in order to make iris inimitable among two persons).
- In other biometric systems like fingerprints, there is a probability of scratches or damage. However, the iris is cosseted behind eyelid, cornea and aqueous humor due to which it becomes very less vulnerable to damage.
- Iris does not deteriorate with aging.
- The use of contact lenses or spectacles does not affect the iris structure's automated reading.

II. LITERATURE REVIEW

The recognition of iris with the help of iris features has gained attention and attracted many researches who gave various approaches in literature work.

Initially, Daugman proposed iris biometrics in 1994. The early publications and patent of Daugman 1994 [2] became a standard reference model. The iris's diameter and center were detected with the help of Integro-differential operators. The image is transformed from Cartesian coordinates into polar coordinates and the area of interest's rectangular representation was engendered. In order to create iris codes, the 2D Gabor wavelets are utilized by feature extraction algorithm and these are matched with the help of Hamming distance. By using the algorithm, the precision of more than 99.99% was achieved. Moreover, the time period in which iris is identified is less than one second.

Wildes defines [3] the outcomes of 2 experimental assessments of technique, consisting of images from numerous irises. The presented paper defines that various different approaches are present for iris biometric system's every main module.

Wildes' [4] technique consists of calculating a binary edge map and subsequently, a Hough transforms for identifying the circles.

Tan et.al. [5] proposed various approaches and after that presented a contrast of various algorithms and techniques of iris recognition.

M. Vatsa et. al. [6], [7], [8], [9] introduced a new iris verification algorithm that makes use of iris image's topological and textural traits. In order to haul out the textural data, the proposed 1D log Gabor wavelet was utilized, and to haul out the topological data from an image of the iris, the Euler numbers were utilized.

For feature extraction, the 2D wavelet transform and Gabor filters were utilized by Zhu et. al. [10] and the weighted Euclidean distance classification was utilized for the identification.

In [11] Z.Z. Abidin et al. introduced a feature extraction approach that depends on epigenetic features utilizing various edge detection operators. For feature extraction from the iris, the Edge detection operators such as Prewitt, Sobel, and Canny were implemented.

In [12] Song et al. presented a technique that depends on the sparse error correction model, while the noise factors such as, eyelash and eyelid occlusion and pupil and specular reflections are primarily spatially restricted.

III. PRESENT WORK

Traditional techniques provide protection to the template by using an image to hide the actual template. This technique is not much secured due to hiding the original data. Also, in order to authenticate the identity of an individual, it is required that the calculated iris template must match with the stored template, and in the conventional approaches matching algorithm that is used is Hamming Distance. Furthermore extracted images were hidden into the cover image without any compression which leads to high variations in the pixel's value.

Therefore, Due to afore mentioned limitations, a new technique has presented in this paper. In the proposed work, bitmask compression technique is used that provides compression to the template. This technique helps in reducing the actual size of the image which ensures that more data can be used to hide and fewer variations will be performed in the pixels of the image. Also, the Support Vector Machines (SVMs) technique is used as a pattern matching method to verify a person's identity based on the iris code.

In proposed work, as shown in fig. 2 to fig.5 below, first of all, the iris image is selected and then the template is created for the selected iris image and then the cover image is selected. After selecting the cover image, the data hiding operation is performed on the template. And finally, the stego image is achieved.

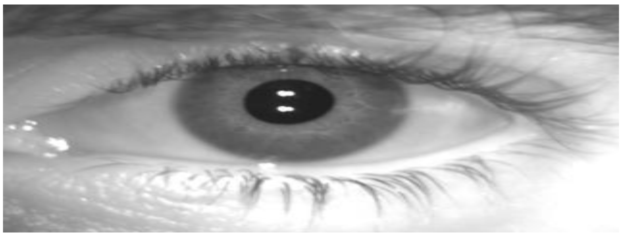

Fig. 2. Iris image

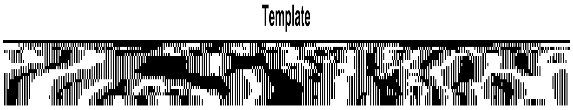

Fig. 3. Template

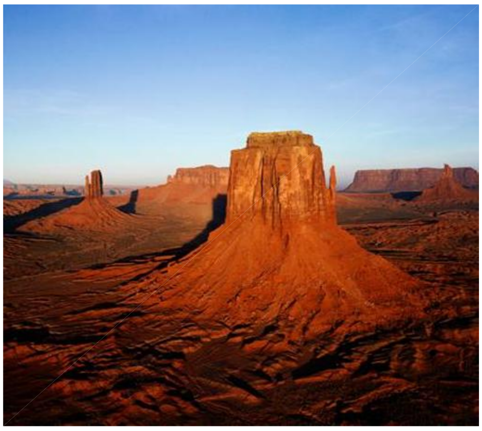

Fig. 4. Cover Image

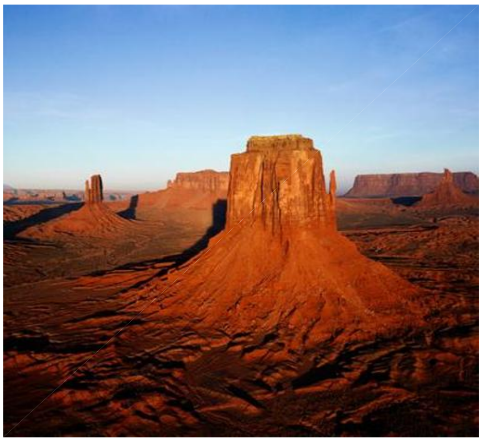

Fig. 5. Stego Image

IV. RESULTS AND DISCUSSIONS

In this section, the results of proposed work are delineated. The presented model is designed with the aim of maintaining the security of the iris template to make the database consistent and confidential. In the given proposed technique, performance parameters are considered to measure the accuracy, efficiency and proficiency of a particular technique. The various parameters used are GAR, PSNR, MSE and BER. The results obtained are described below:

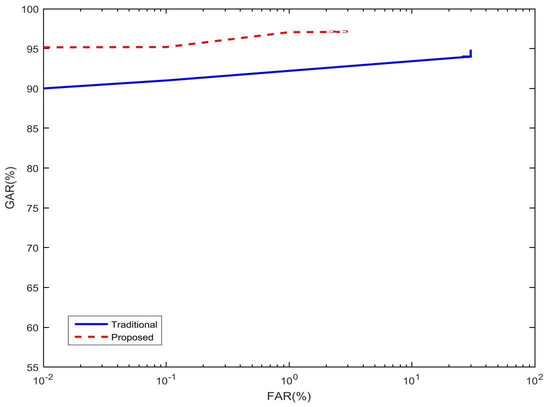

Fig. 6. ROC curve for GAR vs. FAR

In fig. 6, Receiver Operating Characteristic (ROC) curve is plotted for the Genuine Accept Rate (GAR) against False Accept Rate (FAR) to check the efficiency of the proposed approach. FAR is the proportion of fraud pairs whose match score is greater or equal to the prescribed threshold value. The GAR is the fraction of genuine scores greater than the threshold value. The graph depicts that the proposed system obtains considerable results as it has greater GAR value than the conventional approach. Thus, it can be stated that the recognition in designed approach is enhanced to a great extent.

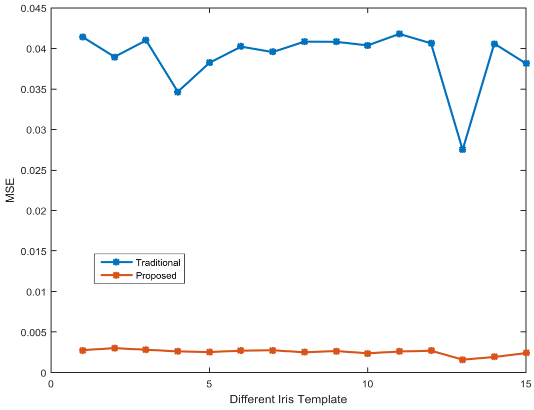

Fig. 7. Mean Square Error of traditional and proposed approach

The graph in fig. 7 compares the mean square error achieved for both proposed and existing methods. It is the difference of the estimator and the estimated value. The graph demonstrates that the error in the proposed work is comparatively very less than that of traditional method which in turn ensures the efficacy of the novel method.

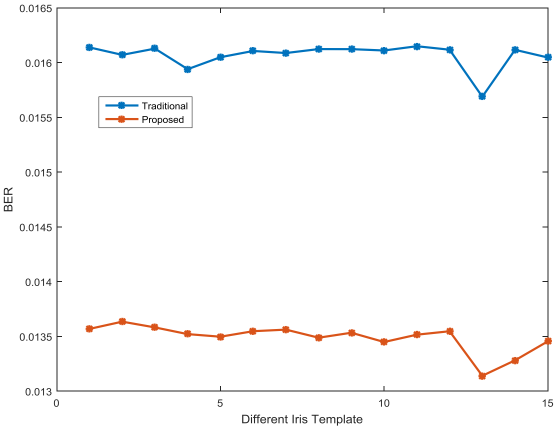

Fig. 8. Bit Error Rate of proposed and traditional approach

The graph represented in fig. 8 demonstrates the comparison the value of Bit Error Rate (BER) of the proposed and conventional work. BER attained for proposed work is less than that of conventional method. As less BER gives higher effectiveness, the projected approach is countered to be better than existing approach in terms of BER. The results for Peak Signal to Noise Ratio (PSNR) are delineated in the fig. 9. It presents the ratio between the maximum signal (original data) and the noise (error in the data).

The graph represents that PSNR for proposed work is higher which increases effectiveness of designed method.

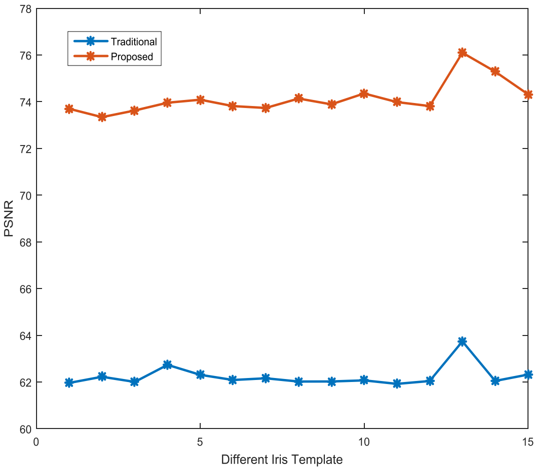

Fig. 9. Peak Signal to Noise Ratio of proposed and traditional approach

Thus, all of these results demonstrate that as compared to the traditional technique, the proposed one is countered as more efficient for the iris template security.

V. CONCLUSION

A novel approach is proposed to secure the iris template in which a bitmask compression technique is employed to compress the actual size of the template making the hiding process easier. The purpose of employing compression technique is to avoid data hacking. Besides this, in order to verify the identity of an individual based on the iris code, the SVM technique is used as a pattern matching technique. The simulation of the proposed system is performed for which various performance parameters are considered such as, GAR, PSNR, MSE and BER.

The simulation results ensure the high security of the iris template as the proposed technique attained higher PSNR and GAR and low MSE and BER as compared to the traditional approach.

REFERENCES

1. https://www.bayometric.com/biometric-iris-recognition-application/
2. John Daugman, “Biometric Personal Identification System Based On Iris Analysis”, 291,560, 1994.
3. Wildes R.P., “Iris Recognition: An Emerging Biometric Technology”, Proceeding of IEEE, Vol.85, issue no. 9, 1997.
4. Richard P, Wildes Jane C, AsmuthKeith J, HannaStephen C, HsuRaymond J, Kolczynski James R, MateySterling E. McBride, “Automated, Non-Invasive Iris Recognition System and Method”, U.S. Patent No. 5,572,596 and 5,751,836, 1996 and 1998.
5. A. A. Kassim, T. Tan, and K. H. Tan, “A Comparative Study Of Efficient Generalized Hough Transform Techniques”, Image and Vision Computing, 1999, vol. 17 pp. 737-748.
6. MayankVatsa, Richa Singh, and P. Gupta, “Comparison of Iris Recognition Algorithms”, International Conference on Intelligent Sensing and Information Processing, 2004 pp. 354–358.
7. MayankVatsa, Richa Singh, and AfzelNoore, “Reducing the False Rejection Rated Of Iris Recognition Using Textural And Topological Features”, International Journal of Signal Processing, 2005, vol. 2, issue no. 2. pp: 66–72.
8. MayankVatsa, Richasingh, AfjalNoore, “Integrating Image Quality In 2ν-SVM Biometric Match Score Fusion”, International Journal of Neural systems, 2007, Vol. 17, issue no.5, pp 343-351.
9. Mayankvatsa, Richasingh, AfzelNoore, “Improving Iris Recognition Performance Using Segmentation, Quality Enhancement, Match Score Fusion, And Indexing”, IEEE trans. On systems, man and cybernetics, Part B , 2008, Vol, 38, No 4, pp. 1021-1035.
10. K. M. Ali Alheeti, “Biometric Iris Recognition Based on Hybrid Technique,” IJSC., 2011, vol. 2, no. 4, pp. 1–9.
11. Z. Z. Abidin, M. Manaf, A. S. Shibghatullah, S. Anawar, and R. Ahmad, “Feature Extraction from Epigenetic Traits using Edge Detection in Iris Recognition System,” IEEE Int. Conf. Signal Image Process. Appl., pp. 145–149, Oct. 2013.
12. Song, Yun, Wei Cao, and Zunliang He. "Robust Iris Recognition Using Sparse Error Correction Model and Discriminative Dictionary Learning." Neurocomputing, 2014, vol 137, pp: 198-204

AUTHORS PROFILE

Monis Khan (M.Tech Scholar) Jagannath University Jaipur, India.
MBA (IT), CDAC MOHALI (TRAINEE), ABV-IIITM GWALIOR (Got Excellent award in Advance IT Professional Training), CCNA.

Suraj Yadav (M.TECH) Associate Professor, Jagannath University, Jaipur , India.