International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Iris Image Authentication using Visual Cryptograph

V.Udayini, Ch.Hima Bindu, P.Naga Malleswari

Abstract*: *In this paper, "Iris Image Authentication using Visual Cryptography", we are using cryptography Technique to authenticate iris template which is quite easy when compare to other types. Hence in this iris authentication we are using circular Hough transform for the extraction of pupil from the eye. Then the extracted features are used for cryptography for accessing of the data. In the proposed work, initially the iris image database images are trained using segmentation, normalization, hough transform and feature extraction process respectively. Later the text image is applied to acquire the features of the matched iris image form the database. The training and texting time of the image is measured based on the size of the database.

***Index Terms*: *Visual Cryptography, Segmentation, Normalization, Hough Transform, Feature Extraction*.**

I. INTRODUCTION

Bio metrics is a technology that is used to authenticate the identity of the person with behavioral characteristics [26]. These types of Bio metrics are helpful in passport verification purposes, to login in to electronic devices, E-commerce, Border crossing, ETC. There are different types of techniques which are cryptography, stenography, watermarking etc for authentication of bio metrics [2, 3, 5, 6, 7]**.** Bio metrics are very Easy & Consistent. Few techniques which are finger print, palm print, face recognition etc among all these, iris authentication is one of the most favorable because of its uniqueness, noninvasiveness, stability eye [1]. Still there are some complications about the security fact of both biometric system and biometric data, Centralized data is stored as an template & have an chance of too many attacks. So, now we have to consider the alternative mechanisms. Now, there are different types of researches have been made to protect the data of humans data & template by using visual cryptography. In this paper we are proposing the techniques which can be further processed by visual cryptography. This Cryptography method is applied to iris template to make more secure from kind of attacks in extra layer of authenticity & as well as in centralized data base to the users [8, 9].

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author
V.Udayini*, Department of ECE, QIS College of Engineering &Technology, Ongole, Andhra Pradesh, India.
Ch.Hima Bindu, ECE Department, QIS College of Engineering &Technology,Ongole,AP,India.
P.Naga Malleswari, Sasi Institute of Technology & Engineering, Tadepalligudem, AP, India.

John introduced the first algorithm to perform this iris recognition & his first paper too & live demonstration on this iris bio metrics. The basic concept behind this bio metric has a Longer history and now in these days this results to gains many scientific contributors. In 1953, F.H. Adler who is a British philosophist "According to his inventions he described that the marked iris as distinctive & that particular images are useful for the identification purpose. Instead of finger prints, faces, other bio metrics adler referred this iris bio metrics. Too many researchers had been researched on this iris template & data [11]. Kalka [4] described about the error correcting codes in designing a secure biometrics for control access. The work which is as follows by water & fuel proposed the different ways of establishing the code & detecting the error detecting codes & it approaches called as fuzzy commitment**.**

II. PRELIMINARIES

A. Enrollment

The administrator will collect the eye images as shown in Fig. 1 & then access to secure resources as shown in Fig.2.

Fig.1: Acquisition of Eye image

This Enrolled image is to be processed for further steps. Later on iris is extracted from eye image & step by step process is performed as shown in algorithm. The figure 2 explains basic operation of visual cryptography.

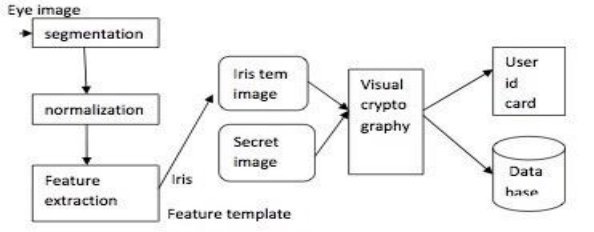


Fig 2: Encoding a binary pixel into 2 shares

i. Segmentation

Segmentation is used to extract the iris from the eye image as shown Fig.3. By performing the circular Hough transform, boundaries of iris is searched.

By fitting two lines using the linear Hough Transform eyelids are detected and eyelash is separated by threshold technique.

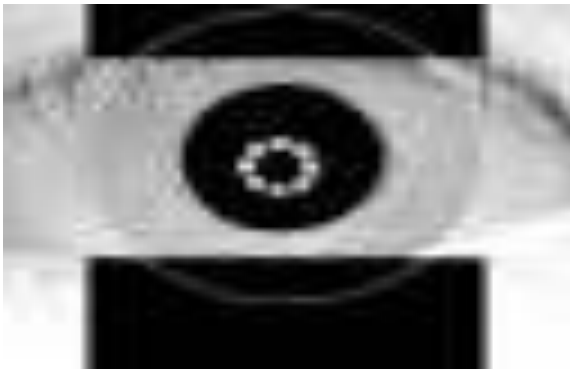


Fig.3: Segmentation of iris

ii. Normalization

In Normalization technique we are using Daugman's model which extracts the pupil of eye & pair of polar coordinates as shown in Fig.4. Pupil, which at the centre is considered as reference point through this iris region [10].

Fig.4: Normalization of iris

iii. Feature Extraction

In this Feature extraction, we convolve the normalized iris pattern in to 1-D Log- Gabor wavelets as shown in Fig.5. The resultant information for both the imaginary & real responses are generated, quantized a bitwise template which is in appropriate sizes (as per given eye sizes).

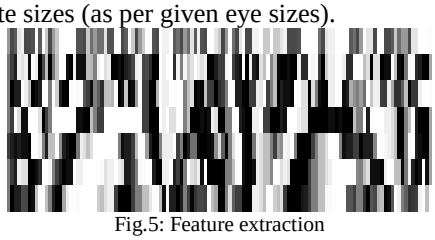


Fig.5: Feature extraction

B. Authentication

In this, Authentication process user will provide the shares in different forms such as id cards. Then the system will finds share from data base. After that a new eye image is supplied by the user as shown in above figure. The 3 steps which are mentioned will be processed one by one. If the distance is zero then it matches perfectly and gives the details of the original database. If not it gives the information that the two images are not matched.

III. PROPOSED ALGORITHM

The proposed algorithm is framed in the following steps:

Step 1: Read the input images from database of IRIS

Step 2: Apply segmentation on the above image using Otsu threshold.

Step 3: The segmented image is normalized using daugman's model.

Step 4: Extract the features from the normalized images. These features are stored for further training.

Step 5: Now apply the testing process to extract the text matched features of the text image with the available database image. For this measure the Euclidian distance between the test image and the trained image.

Step 6: Make a decision based on the obtained result.

The flow chart of proposed work is shown in Fig.6.

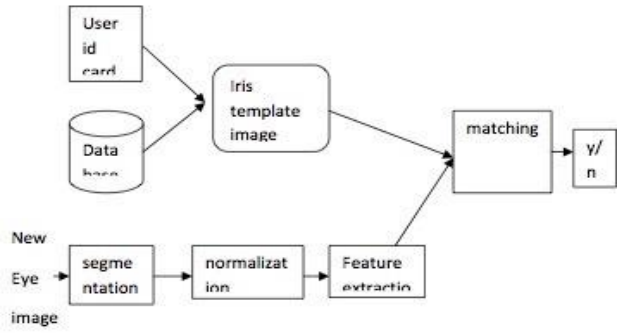


Fig.6: Flow chart of proposed method

IV. IMPLEMENTATION RESULTS AND DISCUSSIONS

The iris image database is collected from [12]. The results of the proposed algorithm are shown in Fig.7 & 8 and the screen shots of the work are given in figure 9. The information is related to matched are not matched to the database. The proposed algorithm is texted about 10-20 database iris images. Each database consists of nearly 20 images. The proposed work executed in MATLAB platform. The execution time is measured based on the database size and tabulated in table I.

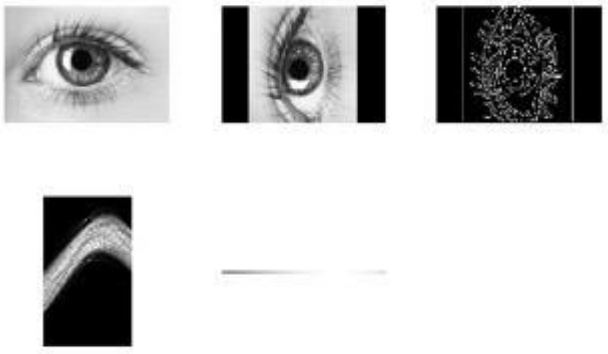


Fig. 7: Results of Image –I: Input Image, Rotational Image, Segmented Image, Hough Transform, Feature Vector Respectively.

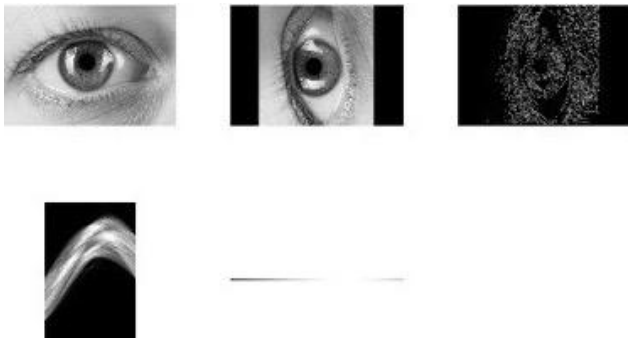
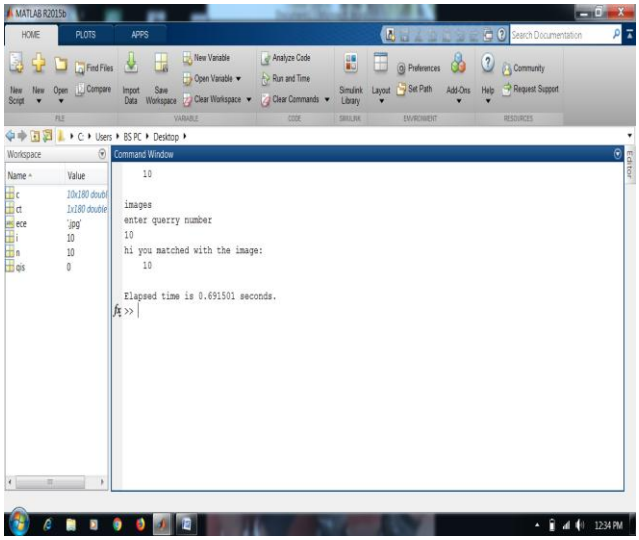
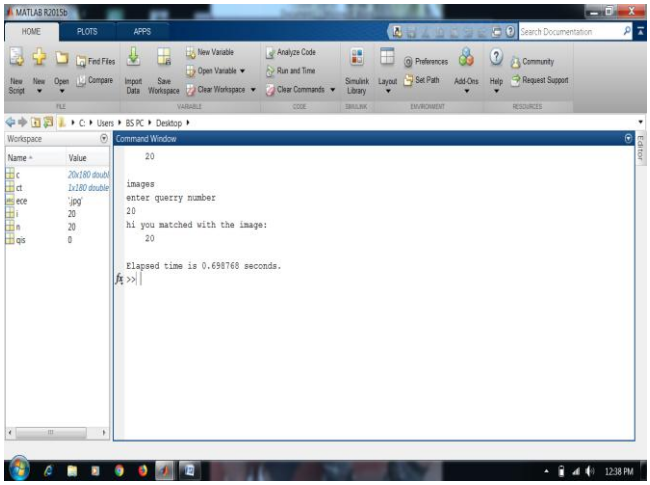
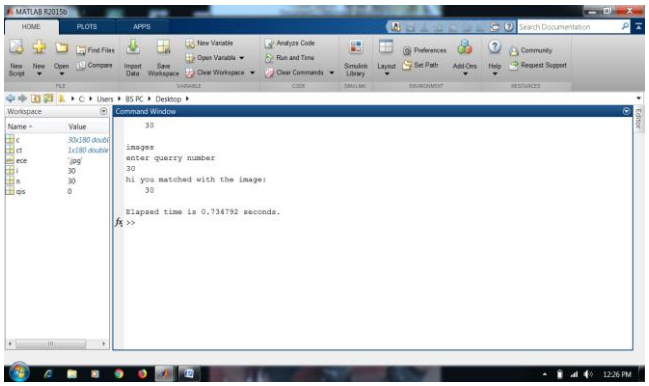
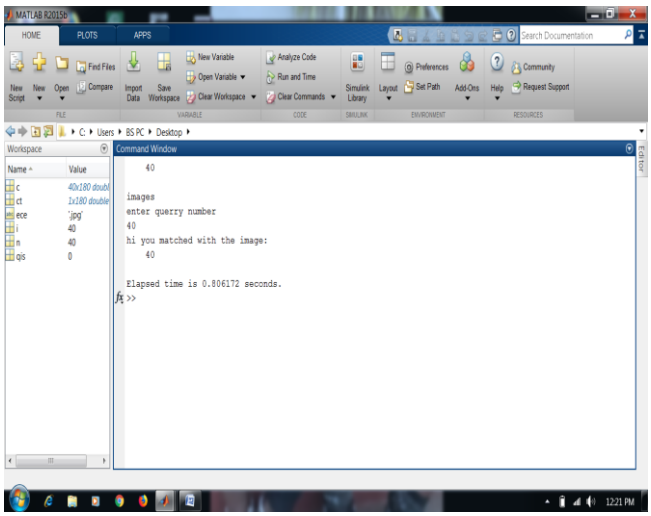


Fig. 8: Results of Image –II: Input Image, Rotational Image, Segmented Image, Hough Transform, Feature Vector Respectively.









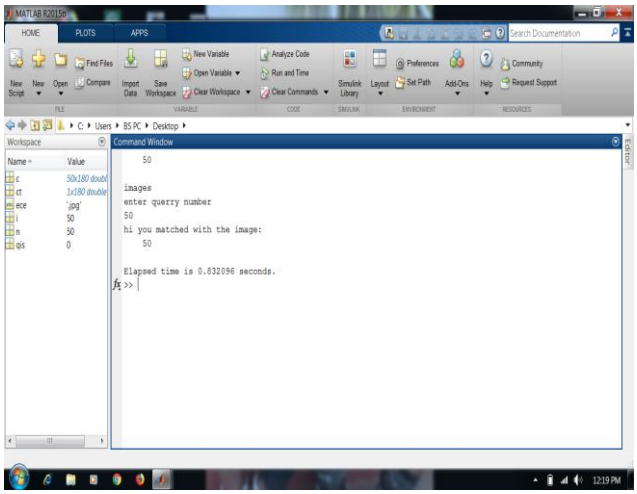


Fig. 9: Screen shots of Output cases in Training & texting Process.

Table I: Number of Images vs. Time

No. of Images in IRIS database	Time of Execution
10	0.601501 Sec
20	0.698768 Sec
30	0.734792 Sec
40	0.806172 Sec
50	0.832096 Sec

V. CONCLUSION

Iris authentication is a process to protect the data & provide maximum extent of security for unauthorized persons. The proposed algorithm can be used for hiding different types of data and to secure the iris template in data base by using visual cryptography.

If the database size is increasing the time of execution also increases and vice versa. This work can be extendable with various distance measures and various segmentation techniques to enhance the results and reduce the computational time. It has various applications such as Computer login control, Passport control and secure electronic banking etc.

REFERENCES

1. G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification" .*In Proceedings of the IEEE Symposium on Security and Privacy*, 148–157, May 1998.
2. Chander Kant, Ranjender Nath & Sheetal Chaudhary, "Biometrics security using steganography". *International Journal of Security*, 2(1),1-5.
3. Khalil Zebbiche, Lahouari Ghouti, Fouad Khelifi and Ahmed Bouridane, "Protecting fingerprint data using watermarking*". In Proceedings of the first NASA/ESA conference on Adaptive Hardware and Systems* (AHS'06),2006.
4. Nick Bartlow, Nathan Kalka, Bojan Cukic, and Arun Ross , "Protecting iris images through asymmetric digital watermarking".1-4244-1300-1, *IEEE*, 2007.
5. Shenglin Yang, Ingrid Verbauwhede "Secure iris verification". *In Proceedings ofthe ICASSP*,133-136, 2007.
6. Jing Dong, Tieniu Tan, "Effects of watermarking on iris recognitionperformance". 978–1–4244–2287–6,*IEEE*, 2008.
7. H.-C. Hsu, T.-S. Chen, Y.-H. Lin, "The ring shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing". *In Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan*, pp. 996–1001, March 2004.
8. Lin Kezheng, Fan Bo, Zhao Hong, "visual cryptographic scheme with high image quality". *In Proceedings of the International Conference onComputational Intelligence and Security*, 366-370,*IEEE* ,2008.
9. Haibo Zhang, Xiaofei Wang, Wanhua Cao, Youpeng Huang , "Visual cryptography for general access structure by multi-pixel encoding with variable block size". *In Proceedings of the International Symposium on Knowledge Acquisition and Modeling*, 340-344, 2008.
10. L. Masek, P Kovesi. MATLAB Source Code for a Biometric Identification System Based on Iris Patterns. *The University of Western Australia*.2003.Availablehttp://www.csse.uwa.edu.au/ studentprojectslibosourcecode.html .
11. S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric recognition: security and privacy concerns". *In Proceedings of the IEEE Security & Privacy*, 33-42, March/April 2003.
12. http://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Iris.htm

AUTHORS PROFILE

Dr.Ch.Hima Bindu is a Professor & HOD at QIS College of Engineering & Technology, Ongole, AP, India. She received B.Tech degree from the QIS College of Engineering & Technology in 2003 and M.Tech, Ph.D. degrees from JNTUK, Kakinada in 2008 and 2014, respectively. She joined as faculty in Department of Electronics & Communication Engineering, QIS College of Engineering & Technology since 2003. She is having 15 years of teaching experience and 9 years of research experience. Dr.Bindu has received a grant worth of 12.5 lakhs from AICTE under RPS Scheme during 2013-16 as CO-PI. She has 2 national patents. She published nearly 45 numerous articles related to digital image processing, signal processing, embedded systems etc. in various reputed international journals and conferences.

P.Naga Malleswari is working as an Asst.Professor at Sasi Institute of Technology & Engineering, Tadepalligudem, AP, India. She received B.Tech and M.Tech degrees from ANU, Guntur, AP in 2004 and 2009 respectively. She is having 13 years teaching experience. Her interesting research areas are Comm& Signal Processing, Image Processing. She is a fellow member of ISTE.