International Journal of Current Trends in Engineering & Research (IJCTER)
e-ISSN 2455–1392 Volume 2 Issue 3, March 2016 pp. 204 - 212
Scientific Journal Impact Factor : 3.468
http://www.ijcter.com

Iris Authentication For Security

Nabanita Nath Chowdhary[1], Khan Kaikasha[2], Khan Nilofar[3], Shaikh Nashrah[4]

[1,2,3,4]*Department of Electronics and Telecommunication*
M.H.Saboo Siddik College of Engineering, Mumbai University

Abstract—This paper presented an iris recognition system in order to verify both the uniqueness of the human iris and also its performance as a biometric identification. A biometric system provides automatic identification of an individual based on a unique feature or characteristic possessed by the individual.. The iris recognition system consists of an automatic segmentation system that is based on the Hough transform, and is able to localize the circular iris and pupil region, occluding eyelids and eyelashes, and reflections,. Stegnography technique is used to hide the crypted code with the unknown encryption key like pattern, logo or an image, so only intended receiver can decrypt the iris code. Super resolution techniques have been employed to enhance the resolution of iris images and improve the recognition performance.

Keywords—Biometric, iris, image processing, cryptography, stegnography, security, transaction

I. INTRODUCTION

In this paper we propose a biometric-based Iris[6] feature extraction system[13]. The system automatically acquires the biometric data in Iris Images by using a set of properly located iris[3] scanners. We are considering an iris scanner as a high quality sensor. The combination of biometrics and cryptography[11] is a promising information security technique which offers an efficient way to protect template[4], as well as to facilitate user authentication and key management. Stegnography[12] technique is used to hide the crypted code[11] with the unknown encryption key like pattern, logo or an image, so only intended receiver can decrypt the iris code.

Biometrics[2] are reliable methods for automatic identification of individuals based on their physiological and behavioural characteristics. Among the biometrics, iris has been shown to be one of the most accurate traits for human identification due to its stability and high degree of freedom in texture [1].A significant recognition performance degradation has been demonstrated when the iris image resolution decreases. The iris is so unique that no two irises are alike, even among identical twins, in the entire human population.

Striking with the purpose of the proposed system, we deal with the implementation of this system in a bank ,which in turn provides us with faster and smarter way for transactions[1] which needs no passbook, cheques or any handy document you just need to proceed with your iris, which will process throughout your bank details in the database through iris capturing with a scanner and further secure transmission techniques.

We have proposed a unique authorization method which involves three secure[10] processing stages in the recognization process. First, image processing[13] takes place which is the initial stage to capture an image and process it. Followed by crypting[11] the acquired image for secure recognition and high level security achievement by stegnography[12] of the iris crypted code. Final stage involves the matching process and authenticating the user by decrypting and de-stegnography of the processed template.

II. PREVIOUS WORK

1. 1936: US opthalmologist Frank Burch suggests the idea of recognizing people from their iris patterns long before technology for doing so is feasible.
2. 1981: American opthalmologists Leonard Flom and Aran Safir discuss the idea of using iris recognition as a form of biometric security, though technology is still not yet advanced enough.
3. 1994: US-born mathematician John Daugman (currently a professor of computer science at Cambridge University, England) works with Flom and Safir to develop the algorithms (mathematical processes) that can turn photographs of irises into unique numeric codes. He is granted US patent #5,291,560 for a "biometric personal identification system based on iris analysis" the same year. Daugman is widely credited as the inventor of practical iris recognition since his algorithm is used in most iris-scanning systems.
4. 1996: Lancaster County Prison, Pennsylvania begins testing iris recognition as a way of checking prisoner identities.
5. 1999: Bank United Corporation of Houston, Texas converts supermarket ATMs to iris-recognition technology.
6. 2000: Charlotte/Douglas International Airport in North Carolina and Flughafen Frankfurt Airport in Germany become two of the first airports to use iris scanning in routine passenger checks.
7. 2006: Iris-scanning systems are installed at British airports, including Heathrow, Gatwick, Birmingham, and Stansted. Privacy concerns notwithstanding, hundreds of thousands of traveller voluntarily opt to use the machines to avoid lengthy passport-checking queues.
8. 2009: Iris authentication for e-commerce along with cryptography chaos theory by Arian Shahriar which provided a boon in security after involvement data crypting techniques. [10]
9. 2016: Previous techniques did provide authentic security in accessing systems but were layed behind in the overall process timing and accuracy. We provide a faster, more accurate, high confidence vision in granting access to a withdrawal statement which involves an amount. Such a system can not only be used in accessing systems but also a real-time system which consist of a considerable amount.The Iris scanner which is used in the initial stage provides with high quality IR vision of a human iris.

III. ALGORITHM

Every Iris recognition algorithm consists of 5 main sections these sections are as follow:

1. Capture the iris image from iris scanner.

2. Extracting iris image and perform adaptive histogram equlization to find region of intrest , then we get the normalized iris image by using 2D-DWT algorithm.

3. Compare data base image with input image using gabor filter[13] and dwt ,if the iris code is identical then the person can proceed for transaction otherwise the access is denied.

4. Then we generate a Unique ID code which consist of 20 bit random number with 5 digit amount no and 1 digit for deposit/withdrawl.so this Unique ID co is encrypted using cryptography technique of rivest sheldman algorithm[11].

5. After cryptography[11] will perform stegnography[12] the result of such combination provides Transmission or achievement of high level security and we get a successful transaction[1].

IV. FLOWCHART

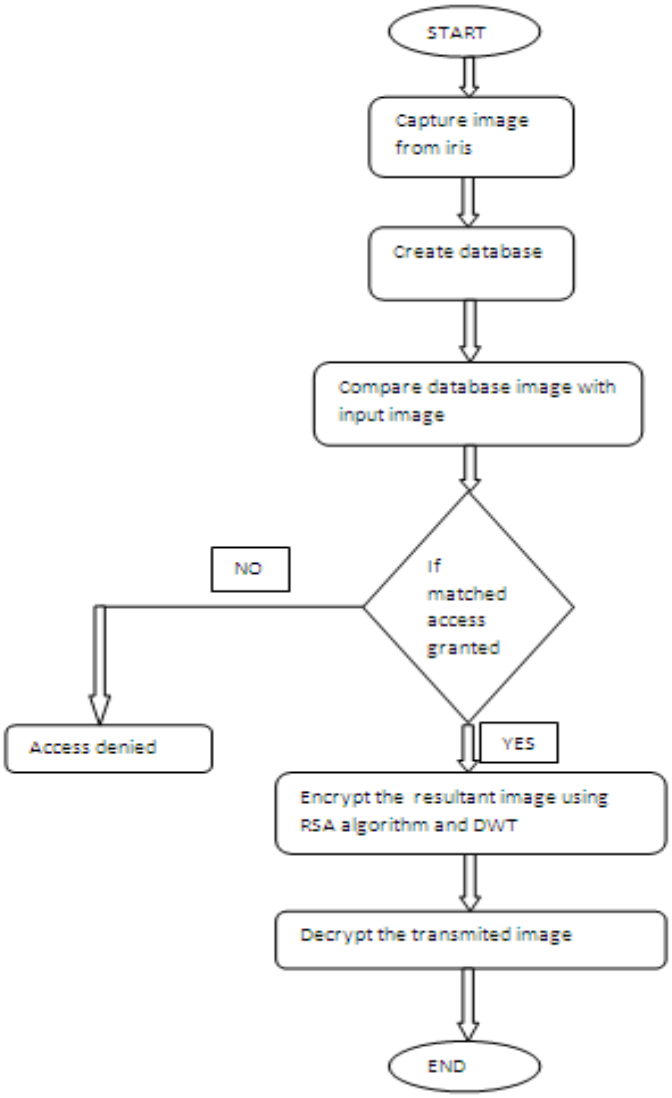


Figure 1: Flowchart

V. ANALYSIS

In this growing world of technologies, today authentication plays the most important role to curb fraudulants and crime. Authentication itself ,is a procedure to verify that a user requesting a resource is who he claims to be! The word 'claim' is a personnel phenomena which gives rise to 'BIOMETRICS'[2] ie 'something that you are', of all the physical and behaivoural identification, strategies or methods, 'Iris recognition[2][3][4] is our preference to the top', since it is an automated method of biometric authentication that uses the process of gathering one or more detailed images of the eye with a sophisticated, high resolution digital scanner of the iris at (IR) wavelengths and then using a specialized program called a matching engine to compare the subjects iris pattern with those images which are stored in our database.

For this matching process or verification a template is created by imaging an iris compared to stored template in the database. The process or image processing to recognize the iris pattern Daughmans algorithm[3], a gabor wavelet transform is used. The result is a set of complex numbers that carry local amplitude and phase information about the iris pattern .In Daughman[2][3] algorithm most amplitude information (complex sign bits of gabor wavelet projection) and discarding the amplitude information ensures that the template remains largely unaffected by changes in

illumination or camera gain and contributes to the long term usability of the biometric template is what matters where it is used any application, be it e-commerce, banking, activation of your identity.

The transmission of the matched templates is done by a promising feature of the combination of biometrics with cryptography which offers information security technique in an efficient way to protect the iris template as well as fascillitate the user authentication and key management, cryptography process of protecting the template is done by the RSA algorithm and followed by steganography[12] which is used to hide the crypted code with unknown encryption key which is used to hide the crypted code with unknown encryption key which may be an image or text.

VI. BLOCK DIAGRAM

Fig :Training/Testing &Application

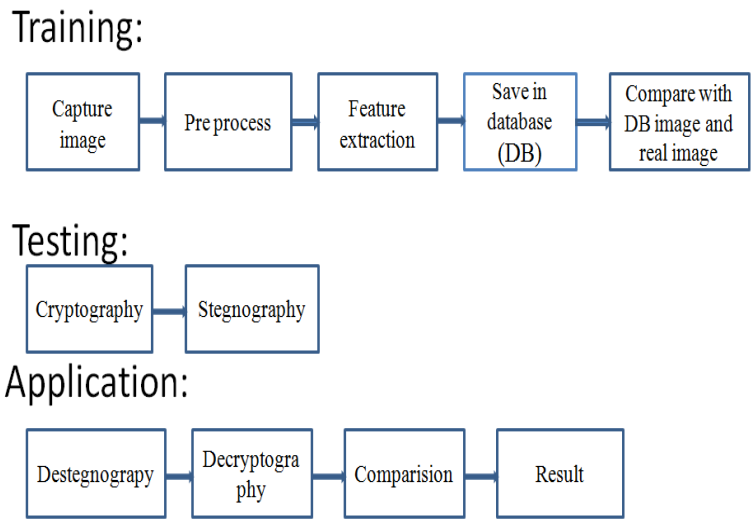


Figure 2: Block diagram

Steganography vs. Cryptography

Cryptography[11] is the science of encrypting data in such a way that one cannot understand the encrypted message, whereas in steganography the mere existence of data is concealed, such that even its presence cannot be noticed. Using cryptography might raise some suspicion whereas in steganography the existence of secret message is invisible and thus not known. We can think of steganography[12] as an extension of cryptography[11], and it is commonly used under the circumstances where encryption is not allowed. Here we are taking 1 image it would be any image we send our secret data to receiver in a image but other person can see only the image not a secure data. This stegnography technique can be perform by DWT.

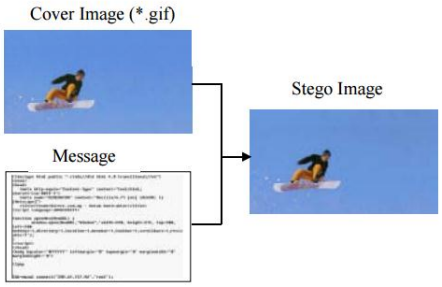


Figure 3: Stegnography

Discrete Wavelet Transform (DWT) Steganography

In this technique DWT is used to separate high frequency components from low frequency components and then replacing the high frequency part by secret data. The embedding capacity of this technique is far greater than DCT steganography[12].

In this project my task is to take secret information as a data file and as an image and to do comparisons between them in terms of embedding capacity and quality of produced stego-image and robustness to attacks.

MATLAB is used as simulator to implement the techniques of steganography[12]. MATLAB provides highly computing environment and advanced in-built function for image processing.

DWT – Stegnography.

1. [A,B,C,D]=dwt(input_image)

This is the original input image on which 2D DWT is performed.

2. [A,B,C,D]=data_string[P,Q,R,S]
   =[A1,B1,C1,D1]

This is the attachment of secret message or data along with the original image.

3. Image1=idwt[A1,B1,C1,D1]

STEP 1: Take DWT of original image.
STEP 2: Hide message string in approximate co-efficient.
STEP 3: Take idwt we get new image, that is the steganographic image with hidden string of message.

VII. ENCRYPTION

Encryption is done by RSA[11] & DWT algorithm. RSA is currently used in wide variety of products, platforms and industries around the world. RSA[11] can be found in secure telephone on Ethernet network cards & on smart cards. RSA is incoprated into all of the major protocols for secure internet communication, including s/MIME,SSL & S/WAN. We are using this RSA algorithm for cryptography for encrypting the iris code, followed by stegnography[12] process to have more security of the transmitted image or data.

VIII. DECRYPTION

Decryption is done at the receiver side, to encode the iris code for further transaction process. The whole encryption and decryption process is carried out with the most authentic transmission processes like RSA\DWT[11][12],which provides us with high security and authenticity.

IX. TRANSACTION

A well authorized graphical user interfaced bank website or any transaction application website may use this iris recognition system for authentic transmission[1]. We have used a bank transaction GUI in which we have all the identifiction details of the account holder along with the iris image in the database. When a particular user wants to access transaction into his account he has to first capture his iris. This image will be matched in the database. If the image is matched the user is granted further access into his account with the user details being displayed as well has his account details. If the image is not matched, the user is denied further access. A user who is granted access, if

he wants to transfer some amount into an account ,he can do so and during this process the encrytption and decryption process takes place.

X. EXPERIMENTAL RESULTS

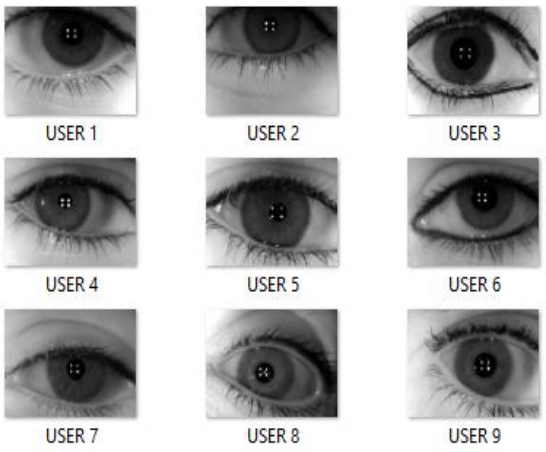


Figure 4: Database Image

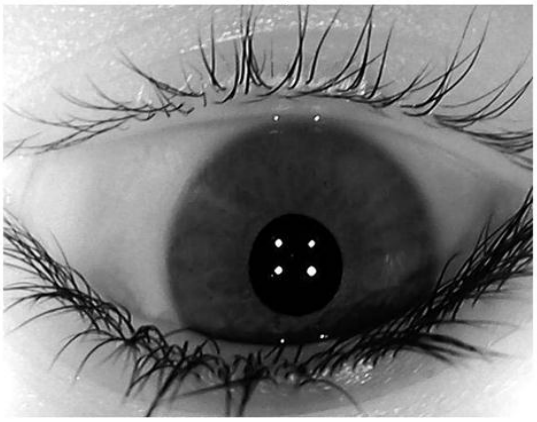


Figure 5: Input image

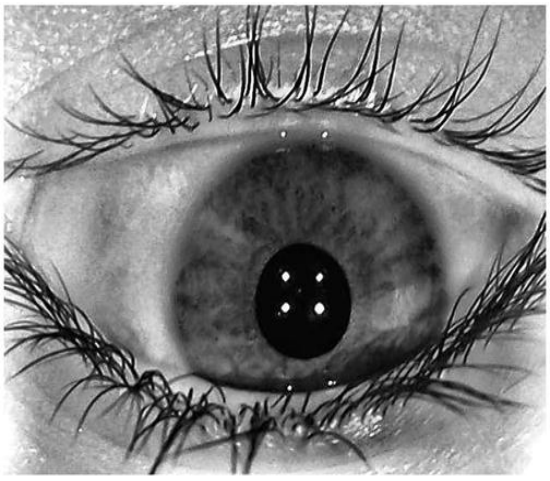


Figure 6: Adaptive histogram equalisation of input image

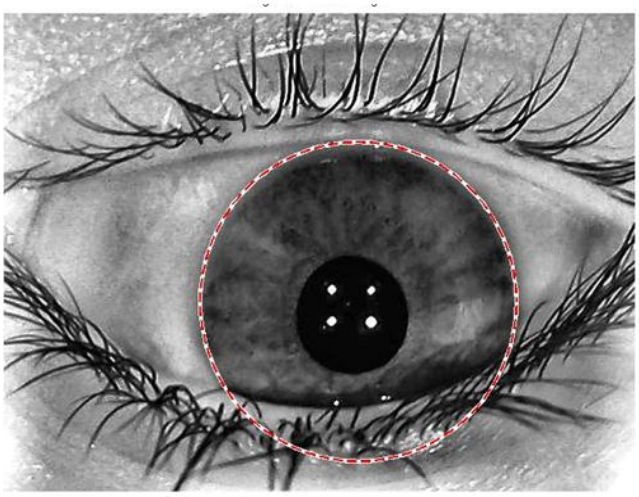


Figure 7: Region of interest image by hough transform.

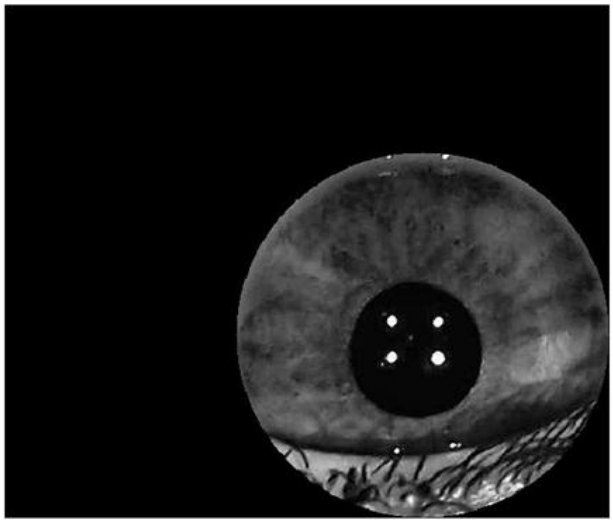


Figure 7: Extraction of region of interest

Figure 8: Normalization of region of interest image

Figure 9: DWT of normalized image

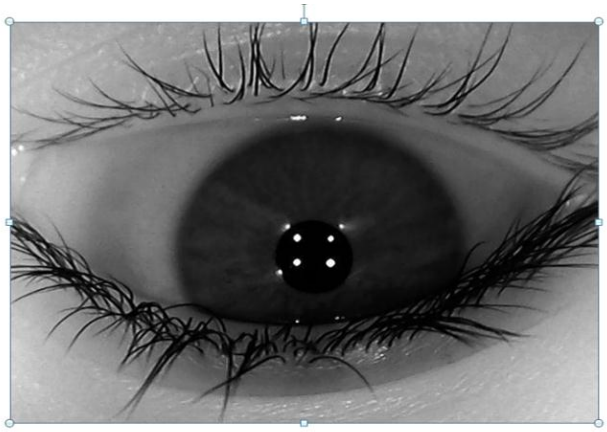
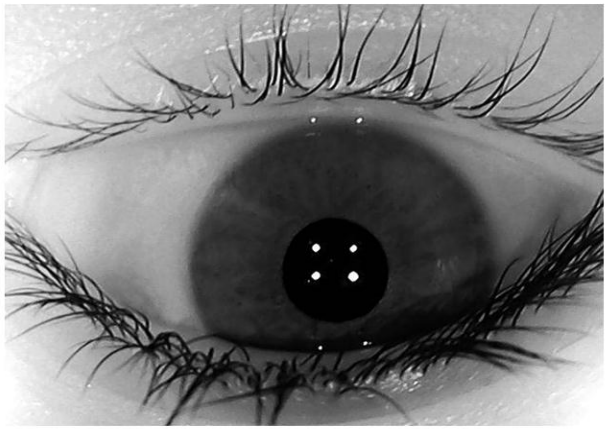


Figure 10: Matched image



Test image

XI. CONCLUSION

The aim of this group project is to implement a working prototype of the techniques and methods used for iris recognition, and to test these methods on our database. The actual application of authenticity of this security system based on iris of humans as a real time based system has been made possible. As well as high level security is achieved through stegnography[12] and cryptography[11] process. The application is not limited to bank transaction only, it is applicable to

attendance system, security access system, e-commerce[10]etc. This system is more authentic and faster than other iris recognizing system existing till today.

REFERENCE

[1] Vagala,R.R, Sasi,S., 'Biometric Authentication for e commerce Transaction', published in the proceeding of international workshop on Imaging Systems and Techniques(IEEE IST),2004

[2] Daugman JG (1993) High confidence visual recognition of persons by a test of statistical independence. IEEE-PAMI, 15: 1148-1161.

[3] Daugman JG (2002) How Iris recognition works. The Computer Laboratory, Cambridge, Iridian Technologies, U.K.

[4] Daugman J (2003) Demodulation by complexvalued wavelets for stochastic pattern recognition. International Journal of Wavelets, Multiresolution and Information Processing, 1: 1-17.

[5] Daugman J (2004) How Iris recognition works. IEEE Trans. Circuits and Systems for Video Technology, 14: 21-30.

[6] J. M. Colores, V. M. Garcia, A. A. Ramirez and M.H Perez "Iris image evaluation for non-cooperative biometric iris recognition system", MICAI 2011, pp.499 -509

[7] A. K. Jain, L. Hong, S. Pankanti and R. Bolle "An identity authentication system using fingerprints", Proceedings of the IEEE, vol. 85, no. 9, pp.1365 -1388

[8] Rajendra Reddy, Vangala Sreela Sasi, "Biometric Authentication for E-Commerce Transaction", IEEE IST 2004, International Workshop on Imaging Systems and Techniques, Stresa Italy, 14 May 2004

[9] Khan, M.K, Zhang,J., Tian,L., "Protecting Data for Personal Identifiaction ",Sinobiometrics,pp. 629-638,2004

[10] Arian rahimi,Sharhriar mohammadi, Rozita rahimi.," An efficient Iris authentication using chaos theory-based cryptography for e-commerce transactions , IEEE,Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for 9-12 Nov. 2009.

[11] Sung-Ming Yen; Seungjoo Kim; Seongan Lim; Sang-Jae Moon,"RSA speedup with Chinese remainder theorem immune against hardware fault cryptanalysis"IEEE Transactions on Computers Year: 2003, Volume: 52, Issue: 4.

[12] M. R. D. Farahani; A. Pourmohammad A DWT Based Perfect Secure and High Capacity Image Steganography Method Parallel and Distributed Computing, Applications and Technologies (PDCAT), 2013 International Conference on Year: 2013.

[13] W. Li; K. Mao; H. Zhang; T. Chai 'Selection of Gabor filters for improved texture feature extraction' Image Processing (ICIP), 2010 17th IEEE International Conference on Year: 2010

