IRIS Based Authentication for Bank Lockers

Jayesh Shahasane, Shashi Pathak, Mahendra Gupta, Babita Bhagat

***Abstract*- Biometric system used for security purpose. Mostly the biometric system used for individual identification e.g. to scan finger, eye, iris, voice, signature, DNA, and Hand geometry. The main purpose of installing biometric system to minimize crimes and terrorist attack. The methodology of the paper to collect primary data from research, interviews, and human observation case studies. The objective of this research paper to control human theft, and terrorist activity in Pakistan. Iris recognition is known as an inherently reliable technique for human identification. Feature extraction is a crucial step for iris recognition and important task. The extracted features are used for matching. The security is an important aspect in our daily life whichever the system we consider security plays vital role. The biometric person identification technique based on the pattern of the human iris is well suited to be applied to access control and provides strong e-security. Security systems having realized the value of biometrics for two basic purposes: to verify or identify users. In this paper we focus on an efficient methodology for identification and verification for iris detection, even when the images have obstructions, visual noise and different levels of illuminations and we use the CASIA iris database it will also work for UBIRIS Iris database which has images captured from distance while moving a person. Efficiency is acquired from iris detection and recognition when its performance evaluation is accurate.**

Keywords: CASIA iris dataset, MATLAB, Discrete Cosine Transform (DCT); gray scale images, canny edge detection.

I. INTRODUCTION

The latest menaces of security have led to the increased awareness of biometric technologies. Various biometric techniques that deals with automated methods of recognizing a person are face, fingerprints, hand geometry, iris, retinal, and vein. Biometric identification provides a valid alternative to traditional authentication mechanisms such as ID cards and passwords, signature to avoid most of the disadvantages of these methods; it is possible to identify an individual based on who they are rather than what they possess or what they remember. The human Iris is an internal organ of the eye, protected by the eyelid, cornea. The two eyes of one person have independent and uncorrelated iris patterns, as do the four eyes of monozygotic twins, because the detailed iris patterns (unlike color) are epigenetic: they develop during gestation without genetic specification. As the technology is iris pattern-dependent, not sight dependent. moreover, it does not require physical contact with the camera in this way, the health issues are minimized. The objective of this paper was to produce a working prototype application that uses an iris recognition tool using the algorithms in order to implement in an accurate and useful way. Iris recognition systems are available that implement similar algorithms. Generally, there are four major processes for a particular iris recognition system they are image acquisition, iris pre-processing, feature extraction and matching. The project aims at developing a high-level security in bank locker systems by using three levels of security such as something you have RFID card, something you know: password, something you are: biometrics [1]. It mainly reduces the accessing time, when compared with manual based banking system. The iris is a thin circular diaphragm, which lies between the cornea and the lens of the human eye. A front view of human eye,

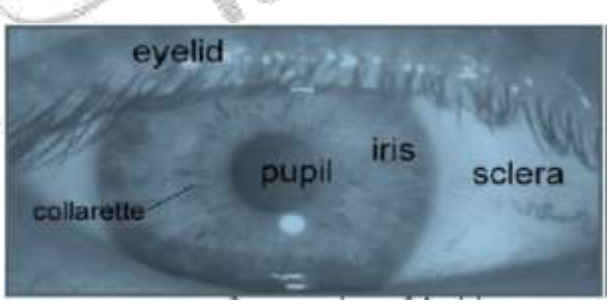

Fig 1. Human Eye

II. BACKGROUND

Biometric authentication, or simply biometrics, offers a natural and reliable solution to the problem of identity determination by establishing the identity of a person based on “who he is”, rather than “what he knows” or “what he carries”. Biometric systems automatically determine or verify a person’s identity based on his

anatomical and behavioral characteristics such as fingerprint, face, iris, voice and gait. Biometric traits constitute a strong and permanent "link" between a person and his identity and these traits cannot be easily lost or forgotten or shared or forged. Since biometric systems require the user to be present at the time of authentication, it can also deter users from making false repudiation claims. Moreover, only biometrics can provide negative identification functionality where the goal is to establish whether a certain individual is indeed enrolled in the system although the individual might deny it. Due to these reasons, biometric systems are being increasingly adopted in a number of government and civilian applications either as a replacement for or to complement existing knowledge and token-based mechanisms. Some of the large scale biometric systems include the Integrated Automated Fingerprint Identification System (IAFIS) of the FBI, the US-VISIT IDENT program, the Schiphol Privium scheme at Amsterdam's Schiphol airport and the finger scanning system at Disney World, Orlando [2]. A number of anatomical and behavioral body traits can be used for biometric recognition. Examples of anatomical traits include face, fingerprint, iris, palmprint, hand geometry and ear shape. Gait, signature and keystroke dynamics are some of the behavioral characteristics that can be used for person authentication. Voice can be considered either as an anatomical or as a behavioral trait because certain characteristics of a person's voice such as pitch, bass/tenor and nasality are due to physical factors like vocal tract shape, and other characteristics such as word or phoneme pronunciation (e.g., dialect), use of characteristic words or phrases and conversational styles are mostly learned. Ancillary characteristics such as gender, ethnicity, age, eye color, skin color, scars and tattoos also provide some information about the identity of a person. However, since these ancillary attributes do not provide sufficient evidence to precisely determine the identity.

III. LITERATURE SURVEY

Iris recognition is a method of recognizing a person by analyzing the random pattern of Iris. Iris recognition has unique, stable and distinctive features for authentication that uses pattern recognition techniques based on high-resolution impersonal identification over age. The difference exists between identical twins and between the left and right eye of the same person. Iris system have a very low false accept rate (FAR) compared to other biometric traits. The false reject rate (FRR) of these systems can be rather high. Image Processing techniques image of the eye encode it into a biometric template, which can be stored in a database. This biometric template contains an objective mathematical representation of the unique information stored in the Iris and allows comparisons to be made between templates.

A lot of research work has been performed in the field of establishing network security based on biometric features obtained from individual user. This section of the paper discusses a few of the related work proposed earlier in association to biometric based network security. In their work Rahman et al., proposed design for secure access of computers inside an organization from a remote location. They used biometrics features and a onetime password method on top of secure socket layer (SSL) for authentication. Furthermore, they also provided three layers of security levels for network communication, and also a mechanism for secure file accesses based on the security privileges assigned to various users is proposed. The files to be accessed from the server are categorized based on their access privileges and encrypted using a key assigned to each category. The test results of their approach evaluated the performance measure of their proposed approach. Chung et al. in described a technique for biometric based secret key generation for protection mechanism. The strap of the user's identity and biometric feature data to an entity is provided by an authority through a digitally signed data structure called a biometric certificate. Therefore, the main objective (or contribution) of their work is to propose a simple method for generating biometric digital key with biometric certificate on fuzzy fingerprint vault mechanism.

IV. IMPLEMENTED SYSTEM

The basic idea of this approach to provide sensor adaptability and to provide high security using multi biometric concepts. I.e. Iris and Fingerprint.

Biometric Authentication process can be stated as:

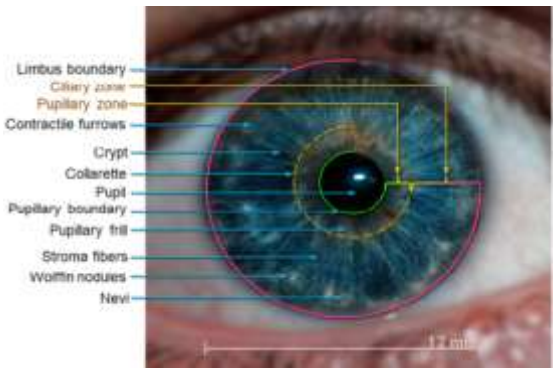

Fig 2. General image of IRIS

1. Image Acquisition

2. Feature Extraction

3. Matching & Decision

Here, we focus on the sensor adaptability as it is not necessary that the sensor used at the time of enrolment is still being used by the system.

The System mainly contains 3 modules:

Iris Recognition

Iris Recognition module is responsible for the enrollment of users‟ iris, learning and sensor adaption and verification process of the user iris [4].

Enrolment Module

Iris Enrolment

The Iris Enrolment procedure has 3 main steps, image acquisition, pre-processing and extracting features and stores them into Database.

Capture the iris image using sensor 1. Apply pre-processing steps on it as follows:

Iris Pre-processing

i. Iris Image Acquisition

For the method we need to test our algorithm on iris images. There are several databases available on the internet, the most famous one being the CASIA database. These are only gray scale images for our method.

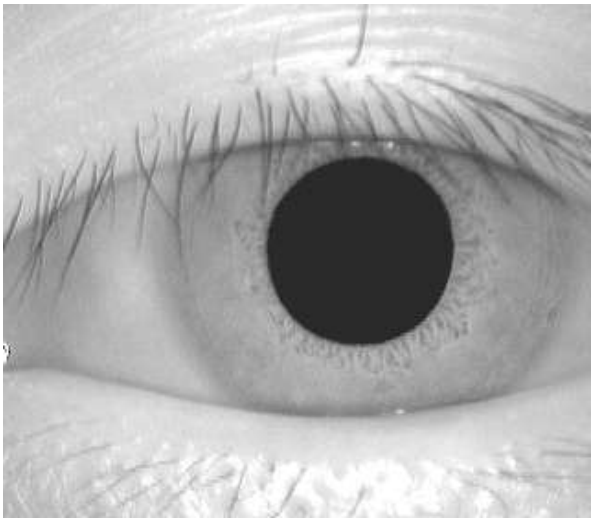

Fig 3. Iris Image in Gray Scale Format

The main features of the Gray database are:

1. The database contains iris images of 10 persons.

2. These are the images of the left eye and there are 3 images each.

3. The images are: 8 bits - Gray, 320 x 320 pixels, .BMP.

ii. Iris Localization & Segmentation

Both the inner boundary and the outer boundary of a typical iris can approximately be taken as circles. However, the two circles are usually not co-centric. The iris is localized in two steps:

(1) approximate region of iris in an image can be found by projecting iris image in horizontal and vertical direction.

(2) the exact parameters of these two circles are obtained by using canny edge detection algorithm.

Canny Edge Detection Steps:

1. Smoothing

2. Finding Gradients

3. Non-maximum Suppression

4. Double Thresholding

5. Edge tracking by hysteresis

iii. Iris Normalization

The normalization process will produce iris regions, which have the same constant dimensions, so that two photographs of the same iris under different conditions will have characteristic features at the same spatial location. Another point of note is that the pupil region is not always concentric within the iris region, and is usually slightly nasal, so remapping is done.

We use Daugman's[3] Rubber sheet model to normalize iris image.

According to this model algorithm, it remaps each point within the iris region to a pair of polar coordinates (r, θ) where r is on the interval [0,1] and θ is angle [0,2π]. 21

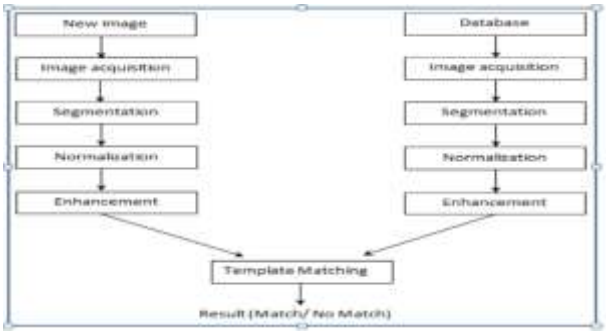

Fig 4. Daugman"s Rubber Sheet Model Mapping of Cartesian co-ordinates into polar co-ordinates

The remapping of the iris region from (x, y) Cartesian coordinates to the normalized non-concentric polar representation is modelled as

$I(x(r, \theta), y(r, \theta)) \rightarrow I(r, \theta)$ ……. (1)

with

$X(r, \theta) = (1\text{-}r)\, xp(\theta) + rxl(\theta)$ ……. (2)

Where I (x, y) is the iris region image, (x, y) are the original Cartesian coordinates, (r, θ) are the corresponding normalized polar coordinates.

Verification Module

Iris Verification

For verification of Iris first the input image of Iris is captured using sensor 2.

Perform the pre-processing steps as mentioned in Iris Enrolment Module.

After pre-processing the iris image, extract features using Log Gabor 1 D filter.

Now Match the extracted features with the Learning and Adaption Parameters stored in the database as follows:

The comparison is done between iris features extracted from captured image and the Features stored in database using hamming distance approach. In this approach the difference between the bits of two codes are counted and the number is divided by the total number of comparisons.

where A is the binary vector for database image and B is the binary vector for query image while N is the number of elements [5].

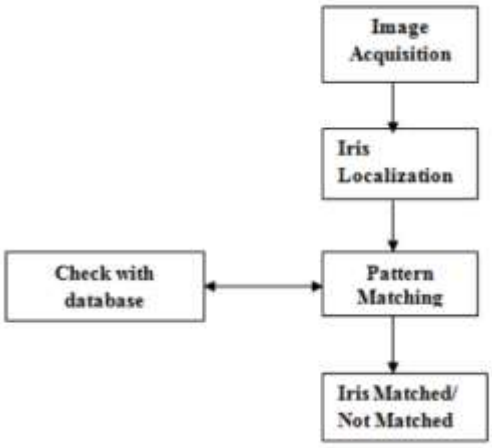

Fig 5. Implemented System Architecture

V. IMPLEMENTED SYSTEM DESIGN

Design Model

Software design is the process by which an agent creates a specification of a software artifact, intended to accomplish goals, using a set of primitive components and subject to constraints. Software design may refer to either "all the activity involved in conceptualizing, framing, implementing, commissioning, and ultimately modifying complex systems" or "the activity following requirements specification and before programming, as a stylized software engineering process.

VI. RESULT

1. The input image to scan iris and to match it with database is selected.

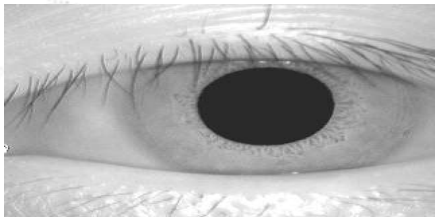

Fig 6. The input Iris image in gray scale

2. The first operation performed on it is resizing of image.

Fig 7. First output is resizing of original input image

3. Draw Circle operation is performed in order to track the iris of the input image.

Fig 8. Second output is draw circle operation on original input image

4. Black and White representation of input image

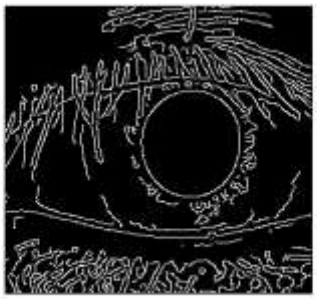

Fig 9. Black and White Representation of original input image

5. It is important to localize that portion of the iris derived from inside the limbus (the border between the sclera and the iris) and outside the pupil.

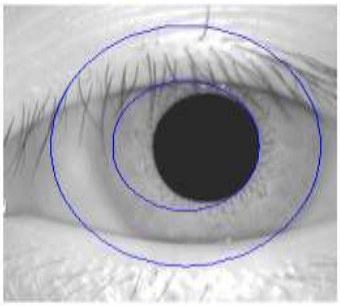

Fig 10. Segmented Iris

6. The input image and the image stored in database is matched with the help of Discrete Cosine Transformation. If the input image and the image in database is matched then it will authenticate the user else it won't give authentication to the user.

VII. CONCLUSION

This paper proposes an approach for information security by means of biometrics. Biometric systems are commonly used to organize accessing of physical assets such as laboratories, buildings, cash from ATMs, etc., or logical information such as personal computer accounts, secure electronic documents, etc. The human biometrics like fingerprint, hand geometry, face, retina, iris, DNA, signature and voice can be effectively used to ensure the network security. In biometric cryptosystems, a cryptographic key is obtained from the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication. In this system, the concept in the areas of image processing technique is reused to extract the minutiae from Iris biometric image. The pre-processing techniques projected in this paper play an important role in improving the performance of the proposed biometric based network security system. The performance measures obtained exposed that the proposed method effectively provides network security. Therefore, it can be directly applied to strengthen existing standard single-server biometric based security applications.

REFERENCES

[1] Mohammad Aakif Kausar, Gautam Purwar, Rajul Raghuwanshi, Prof. Sachin Deshmukh, "User Identification Using Iris Scan",

International Journal of Science, Engineering and Technology Research (IJSETR)

Volume 5, Issue 4, April 2016

[2] Adam Czajka, Senior Member, IEEE, Kevin W. Bowyer, Fellow, IEEE, Michael Krumdick, and Rosaura G. VidalMata, "Recognition of image-orientation-based iris spoofing", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY

[3] J. Daugman," How iris recognition Works," in IEEE Transactions on Circuits and Systems for video Technology, vol.14, no.1, pp21-30, January 2004.

International Journal of Computer Science and Network Security, Vol. 8, no. 10, pp. 14-20, 2008.

[4] Donald M. Monro, Soumyadip Rakshit and Dexin Zhang," DCT-Based Iris Recognition", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, No. 4, April 2007.

[5] Rajeswari Mukesh, A. Damodaram, and V. Subbiah Bharathi, "Finger Print Based Authentication and Key Exchange System Secure Against Dictionary Attack," IJCSNS

[6] Mahfuzur Rahman, and Prabir Bhattacharya, "Secure Network Communication Using Biometrics," IEEE International Conference on Multimedia and Expo (ICME'01), p. 52, 2001.

[7] A. Czajka, "Pupil dynamics for iris liveness detection," IEEE Transactions on Information Forensics and Security (TIFS), vol. 10, no. 4, pp. 726–735, Apr. 2015.