Biometric Security System Using Iris Recognition

Mr. Himanshu S. Bopche Mr. Shubham P. Dube Ms. Pooja P. Khandare Prof. P. D. Pawar

Abstract — **Due to the increasing need for securing data and places, the biometric authentication industry is seeing large market growth. We decided to build a scalable, small, and efficient device that can be used to secure doorways throughout complex. In actual there are many biometric measurements systems that can be used, depending upon the application. Finger print identification is popular biometric technique due to easiness in acquiring, availability and their established use. Whereas the Iris recognition biometric system is complex but having very high accuracy. In our proposed system we decided to use the fusion of these two modalities to provide more reliable, highly secured access to opening closing control system . In this paper we have mainly focused on the principle of iris recognition**

Key Words — **iris, biometric, Daugman**

I. INTRODUCTION

Biometrics, which is formed from the two ancient Greek words bios and metron which mean life and measure respectively, refers to two very different fields of study and application. The first, which is the older and is used in biological studies, is the collection, synthesis, analysis and management of biology. Biometrics uses unique features, like the iris of your eye, to identify you.

To secure the data people typically uses the user names, passwords, and identification cards to prove they are the authorized person for the same. The improved technique that provides reliability and safety in identification and recognition of people is using the Biometric signals. Biometrics signals or identifiers are found to be an essential personal authentication solution, as the biometric identifiers are unique one for every individual and cannot be misplaced or copied in any circumstances .It is implemented in public for commercial purpose. There are many applications of biometrics technology especially in security systems. Each biometric feature has its own strengths and weaknesses and the choice typically depends on the application. The better biometric characteristic has five qualities: robustness, distinctiveness, availability, accessibility and acceptability. Fingerprints are unique and it is most widely used to identify the person. Its matching accuracy was very high . Iris is the ideal part of the eye in human body. It contains many distinctive features such as furrows, ridges and rings etc.

II. LITERATURE REVIEW

Iris recognition technique is one of the biometric verification and identification techniques which also include fingerprint, facial, retinal and many other biological features. They all present novel solutions for human being recognition, authentication and security applications . The iris has been in use as biometric from few decades. However, the idea of automating iris recognition is more recent. The pioneering work in the early history of iris biometrics is that of Daugman. Daugman's 1994 patent and early publications became a standard reference model. Integro-differential operators are used to detect the center and diameter of the Comparative study of iris recognition system using WPNN and Gabor Wavelet Nonlinear Predictive In-line pH c Artificial Neural Computation Literature review on Iris recognition system 15 iris. The image is converted from Cartesian coordinates to polar coordinates and the rectangular representation of the region of the interest is generated. Feature extraction algorithm uses the 2D Gabor wavelets to generate the iris codes which are then matched using Hamming distance (Daugman, 2004). The algorithm gives the accuracy of more than 99.99%. Also the time required for the iris identification is less than 1 Sec.

III. CLASSIFICATION OF BIOMETRICS

Facial Recognition: Facial recognition records the spatial geometry of distinguishing features of the face. Different vendors use different methods of facial recognition, however, all focus on measures of key features of the face. Facial recognition has been used in projects to identify card counters or other undesirables in casinos, shoplifters in stores, criminals and terrorists in urban areas. This biometric system can easily spoof by the criminals or malicious intruders to fool recognition system or program. Iris cannot be spoofed easily.

***Palm Print*:** Palm print verification is a slightly modified form of fingerprint technology. Palm print scanning uses an optical reader very similar to that used for fingerprint scanning; however, its size i much bigger, which is a limiting factor for use in workstations or mobile devices.

Signature Verification: It is an automated method of examining an individual's signature. This technology is dynamic

such as speed, direction and pressure of writing, the time that the stylus is in and out of contact with the ―paper‖. Signature verification templates are typically 50 to 300 bytes. Disadvantages include problems with long-term reliability, lack of accuracy and cost.

Fingerprint: A fingerprint as in Figure1 recognition system constitutes of fingerprint acquiring device, minutia extractor and minutia matcher. As it is more common biometric recognition used in banking, military etc., but it has a maximum limitation that it can be spoofed easily. Other limitations are caused by particular usage factors such as wearing gloves, using cleaning fluids and general user difficulty in scanning.

Iris Scan: Iris as shown in Figure2 is a biometric feature, found to be reliable and accurate for authentication process comparative to other biometric feature available today which is as shown. As a result, the iris patterns in the left and right eyes are different, and so scan be used quickly for both identification and verification applications because of its large number of degrees of freedom. Iris as in Figure 2 is like a diaphragm between the pupil and the sclera and its function is to control the amount of light entering through the pupil. Iris is composed of elastic connective tissue such as trabecular meshwork. The agglomeration of pigment is formed during the first year of life, and pigmentation of the stroma occurs in the first few years

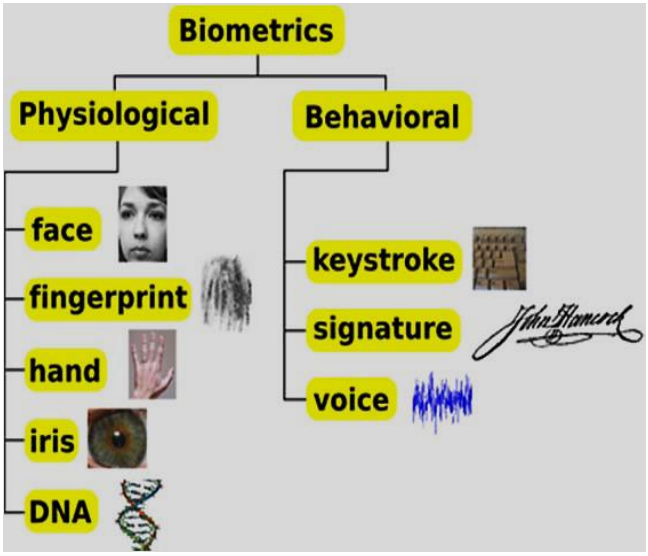


Fig.1 Different Biometric Techniques

1) IRIS SCAN

Iris scanning can seem very futuristic, but at the heart of the system is a simple CCD digital camera. It uses both visible and near-infrared light to take a clear, high-contrast picture of a person's iris. With near-infrared light, a person's pupil is very black, making it easy for the computer to isolate the pupil and iris. The highly randomized appearance of the iris makes its use as a biometric well recognized. Its suitability as an exceptionally accurate biometric derives from

i. The difficulty of forging and using as an imposter person.

ii. It is intrinsic isolation and protection from the external environment;

iii. It's extremely data-rich physical structure.

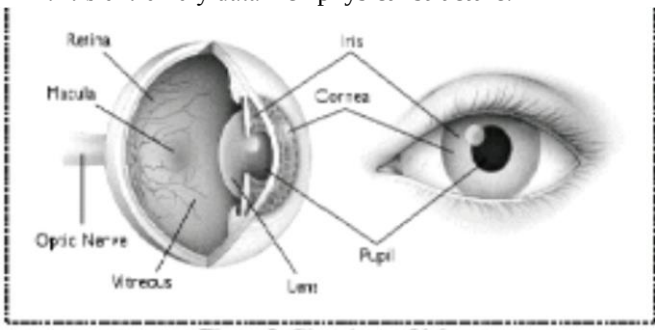


Figure2: Structure of iris.

iv. Its genetic properties—no two eyes are the same. The characteristic that is dependent on genetics is the pigmentation of the iris, which determines its color and determines the gross anatomy. Details of development, that are unique to each case, determine the detailed morphology;

v. its stability over time; the impossibility of surgically modifying it without unacceptable risk to vision and its physiological response to light, which provides a natural test against artifice. After the discovery of iris, John G. Daugman, a professor of Cambridge University suggested an image-processing algorithm that can encode the iris pattern into 256 bytes based on the Gabor transform. In general, the iris recognition system is composed of the following five steps as depicted in Figure 3 According to this flow chart, preprocessing including image enhancement. The remainder of the paper is organized as follows: Section (2) focuses on Image Acquisition Section (3) emphasizes on Preprocessing Section (4) focuses on Feature extraction Section(5) emphasizes on Pattern matching Section(6) emphasizes on identification and verification Section (7) emphasizes on conclusion of the proposed Algorithm.

1) IMAGE ACQUISITION

An image of the eye to be analyzed must be acquired first in digital form suitable for analysis. In further implementation we will be using CASIA database . The main focus CASIA database is to minimize the requirement of user cooperation, i.e., the analysis and proposal of methods for the automatic recognition of Individuals, using images of their iris capture data- distance and minimizing the required degree of cooperation from the users, probably even in the covert mode

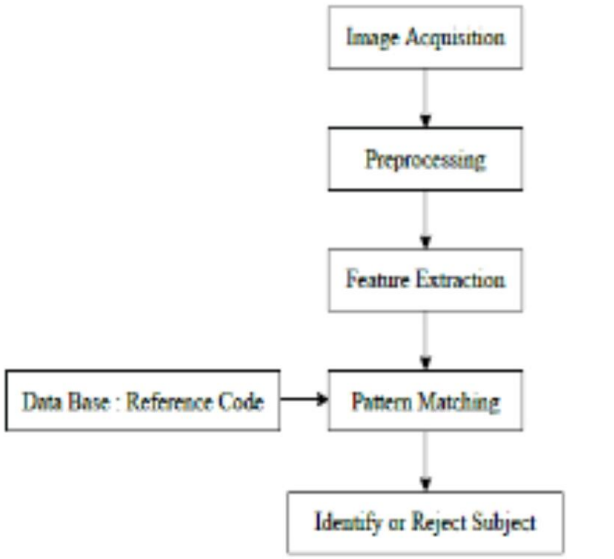


Figure 3: General steps of the iris recognition system

IV. PREPROCESSING

3.1 Algorithm for detection and segmentation

Iris detection

Irises are detected even when the images have obstructions, visual noise and different levels of illumination. Lighting reflections, eyelids and eyelashes obstructions are eliminated. Images with narrowed eyelids or eyes that are gazing away are also accepted using wavelet algorithm. Automatic interlacing detection and correction: The correction results in maximum quality of iris features templates from moving iris images. Gazing-away eyes**:** A gazing-away iris image is correctly detected, segmented and transformed as if it were looking directly into the camera.

Correct iris segmentation::

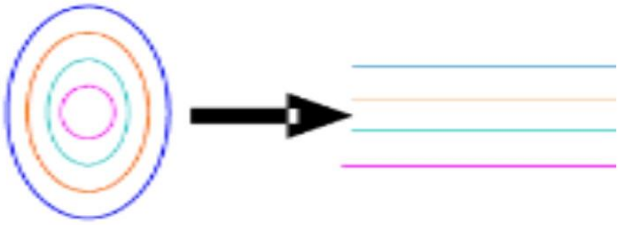


Figure 4: Polar transformation

It is achieved under these conditions

Perfect circles fail. Eye uses active shape models that more precisely model the contours of the eye, as perfect circles do not model iris boundaries. The centers of the iris inner and outer boundaries are *different* Figure8. The iris inner boundary and its center are marked in red; the iris outer boundary and its center are marked in green. Iris boundaries are definitely not circles and even not *ellipses* Figure9.and especially in gazing-away iris images. Iris boundaries seem to be perfect circles**.** The recognition quality can still be improved if boundaries are found more precisely compared to perfect circular white contours.

Locating Iris

The first processing step consists in locating the inner and outer boundaries of the iris and second step to normalize iris and third step to enhance the original image. The Daugman's system, Interco differential operators as in (1) is used to detect the center and diameter of iris and pupil respectively.

max(, 0, 0) 0 $I(r$ *cos $x0, r$ *sin $y0)$ Where (x0, y0) denotes the potential center of the searched circular boundary, and r its radius. 2 Cartesian to polar reference transform Cartesian to polar reference transform suggested by J.Daugman authorizes equivalent rectangular representation of the zone of interest as in (see Figure 4,5) remaps each pixel in the pair of polar co-ordinates(r, θ) where r and θ are on interval [0,1] and [0,π] respectively. The unwrapping in formulated as in (2) where $I(x, y)$, (x, y), (r, θ), (xp, yp), (xi, yi) are the iris region, Cartesian coordinates, corresponding polar coordinates, coordinates of the pupil, and iris boundaries along the θ direction, respectively. (See Figure4) shows polar transformation.

4. FEATURE EXTRACTION

The most important step in automatic iris recognition is the ability of extracting some unique attributes from iris, which help to generate a specific code for each individual. Gabor and wavelet transforms are typically used for analyzing the human iris patterns and extracting features from them,

Steps for feature Extraction:

1 Apply 2DDWT with Haar up to 5-level decomposition

2 Using 4th level, 5th level decomposition details construct the feature vector.

3 Binaries the details getting from step no. 3Store these feature vectors.

V. METHODOLOGY

Security has become a serious issue in areas like airports banks, R&D dept etc where the person entering in the area has to provide his identity. If this identification is performed manually it will be time consuming & too hectic and errors may occur. The system is to be designed to avoid the access of unauthorized person in restricted areas .Security System using iris as biometrics works in following two major steps.

1. Iris recognition system to recognize the person.

2. Iris recognition system integrated with microcontroller & LCD.

The iris recognition system is as shown below

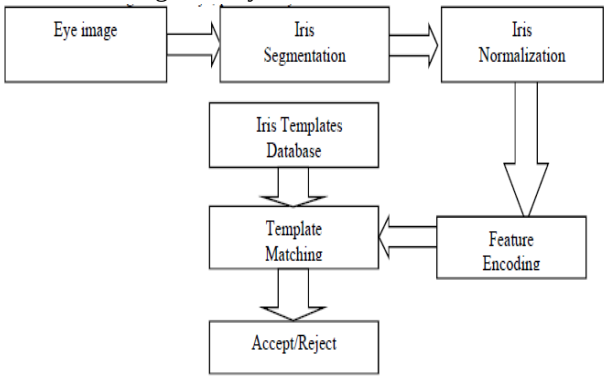


Fig 5 : The iris recognition system

The iris recognition system is basically a five steps process as follows.

1. Iris segmentation
2. Iris normalization
3. Feature Encoding
4. Template Matching
5. Accept/Reject Decision

1. Iris Segmentation:

Captured eye image will act as an input for this stage. It deals with segmenting the part from an eye image. Iris segmentation consists of iris inner and outer boundaries localization, detection of upper and lower eyelids, and detection/removal of reflections from the cornea.

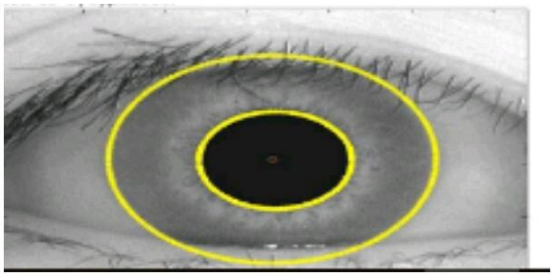


Fig 6 : Iris Segmentation

Fig 6 : Iris Segmentation

2. Iris normalization:

Iris normalization is remapping the segmented iris region to the fixed-size rectangular image by mapping the extracted iris region into normalized coordinate system

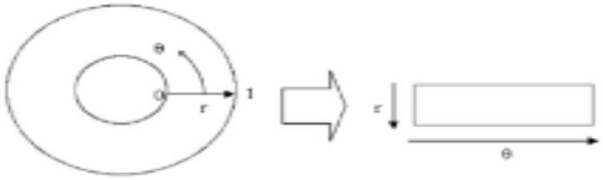


Fig 7 : Iris Normalization

3. Feature Encoding:

In the feature encoding step, a template representing iris pattern information is created using Gabor filter or Log-Gabor filter.

4. Matching:

The goal of matching is to evaluate the similarity of two iris representations. Created templates are compared using the Hamming distance or Euclidean distance

5. Accept/Reject Decision:

In this step, if templates are matched with each other, then human identification will be accepted otherwise it will be rejected. The iris recognition system integrated with microcontroller is as shown in figure

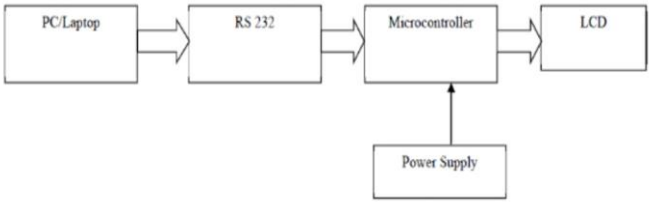


Fig 8 : Block Diagram of Iris based security system using microcontroller

The block diagram consists of the following blocks.

- Personal computer/Laptop
- RS 232 - Serial communication
- Micro controller
- Power Supply
- LCD - (Liquid crystal display)

Personal computer/Laptop: The personal computer /Laptop will contain the iris recognition data of the persons which will be given to microcontroller via serial interface RS232.

RS 232 - Serial communication:

It is used for serial communication between personal computer and microcontroller.

Microcontroller: The microcontroller will receive the serial data from PC & will control the system.

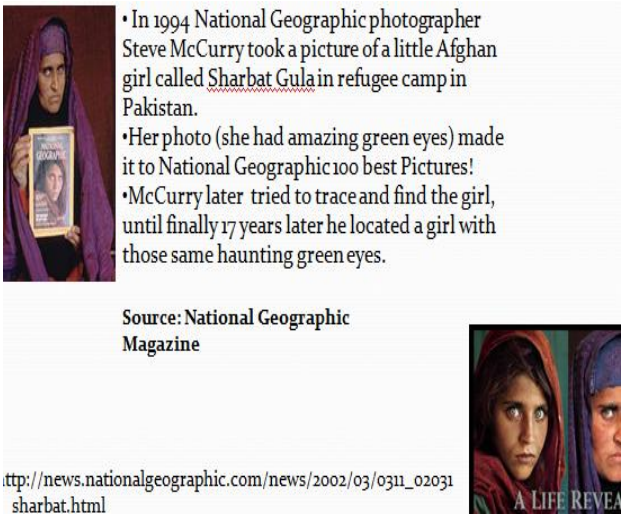
Power supply: The DC power supply requirement for the system will depend on selection of microcontroller.

Liquid Crystal Display (LCD): LCD is used to display the status of the persons. If comparison is true then micro controller will switch on the relay. If the person is recognized then the microcontroller will display "ACCESS IS VALID". If some other person tries to enter, the micro controller checks with database& if it is wrong it displays in the LCD as "ACCESS DENIED".

Advantages

1. No contact required.
2. Protected internal organ, less prone to injury .

3. Believed to be highly stable over lifetime



17 years passed…how to verify if this was the same girl?

- Hard-ship changed the girl's appearance. But she had those same haunting green eyes…
- The Explorer team got verification using U.S.FBI iris scanning technology. They used iris image from old taken photograph and compared to the new one.
- Iris code declared a 'match'!

This was indeed the same girl! Iris biometric made it possible to verify this.

Disadvantages

1. .Difficult to capture for some individuals.
2. Easily obscured by eyelashes, eyelids, lens and reflections from the cornea.
3. Public myths and fears related to "scanning" the eye with a light source and cannot be verified by a human.

Comparison

Method	Coded Pattern	MisIdentific--ation rate	Security
Iris	Iris pattern	1/1,200,000	High
Fingerprint	fingerprints	1/1,000	Medium
voice	Voice characteristics	1/30	Low
Signature	Shape of letters, writing Order, pen pressure	1/100	Low
Face	Outline, shape & distribution of eyes, nose	1/100	Low
Palm	size, length, & thickness hands	1/700	Low

CONCLUSION

"Security system using iris as biometrics" will be able to prevent the access of unauthorized persons in the restricted areas by displaying the information of recognized person & it will also provide error free Biometrics can only be limited by limiting one's imagination. Biometric technology is now being used in almost every area. Although few techniques are discussed in this paper prove to be some of the popular and useful techniques for in the area of biometric recognition.

ACKNOWLEDGMENT

Authors wish to thanks J.D.I.E.T College of Engineering and Technology, Yavatmal, Maharashtra, India. Also like to pay gratitude towards Head of Department, Electrical Engineering and Principal of J.D.I.E.T College of Engineering and Technology, Yavatmal, Maharashtra, India for their valuable support and encouragement.

REFERENCES

[1] Vanaja Roselin.e.Chirchi (ph.d. research scholar) jnt university, kukatpally,hyderabad- 500085. ap, india

[2] Dr. I. M. Waghmare Professor & dean (r&d) sggs institute of engineering &technology, vishnupuri, nanded-431602, ms, India E.R.Chirchi asst. professor, cse dept mbes coe. ambajogai

[3] Harshada terkhedkar and prof. dr. s. l. lahudkar , "person identification for security system using iris biometric technique", international journal of advanced research in computer engineering & technology (ijarcet) ,volume 4, pp 1456-1458 april 2015

[4] Indu verma and sanjay kumar jain, "biometrics security system", ieee 2nd international conference on computing for sustainable global development, pp 1189-1192, 2015