BIOMETRIC SECURITY SYSTEM USING IRIS RECOGNITION

[1]SHUBHAM DUBE, [2]HIMANSHU BOPCHE

[1]UG Student, B.E. Final Year (E&TC), J.D.I.E.T,Yavatmal, SantGadge Baba AmravatiUniv, Maharashtra, India
Lohara Road, Yavatmal (445001), Maharashtra, India
[2]UG Student,B.E. Final Year (E&TC), J.D.I.E.T, SantGadge Baba AmravatiUniv, Maharashtra,India Lohara Road,Yavatmal(445001),Maharashtra, India
Email: [1]sd28167@gmail.com, [2]himanshusbopche@gmail.com

Abstract - As there is increasing need for securing data and places So, The Biometric authentication industry is experiencing large market growth. Therefore, we decided to build a scalable, small, and efficient device that can be used to secure doorways throughout complex. Actually, 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. On the other hand, The Iris recognition biometric system is complex but has very high accuracy. In our proposed system we are using the fusion of these two modalities to provide more reliable, highly secured access to opening closing control system. In this paper we focus mainly on the principle of iris recognition

Index terms - Iris, Biometrics, Stroma, Daugman

I. INTRODUCTION

Biometrics is formed from the two ancient Greek words bios and metron which precisely means life and measure and it refers to two contrasting fields of study and application. Out of which, first one is older and is used in biological studies, which is the collection, synthesis, analysis and management of biology. Biometrics takes into consideration, unique features consisting of the iris of your eye, to identify you. In order to secure the data, It considers the user names, passwords, and identification cards to prove they are the authorized person for the same. It is an improved technique that provides reliability and safety in identification and recognition of people using the Biometric signals. Biometrics signals or identifiers are found to be a pre-requisite for personal authentication solution, as the biometric identifiers are one and only one for every individual and cannot be misplaced or copied in any situation .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 way we apply it. An Ideal biometric characteristic has five qualities: sturdy, distinguishable, availability, covinience and acceptability. Fingerprints are an efficient way used to identify the person. The way it matches with accuracy is very high. Iris is an epitome of the eye in human body. It contains many distinguishable features such as furrows, ridges and rings etc.

II. CLASSIFICATION OF BIOMETRICS

Facial Recognition: Facial recognition records the spatial geometry of distinctive features of the face. Different vendors use various methods of facial recognition, However, all of them focus on key features of the face. Facial recognition is being used in projects to identify card counters or other under-aged in cinemas, shoplifters in stores, criminals and terrorists in urban areas. This biometric system can easily trace the criminals or malicious intruders who fool recognition system or program. Iris cannot be fooled easily.

Palm Print: Palm print verification has taken its roots of use from fingerprint technology. It uses an optical reader which resembles that used for fingerprint scanning; however, its size is much bigger, which is a limiting factor for use in workstations or mobile devices

Signature Verification: It is a method which automatically examines an individual's signature. This technology is zestful 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 ranges from 50 to 300 bytes. Disadvantages includeproblems 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 suchas 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

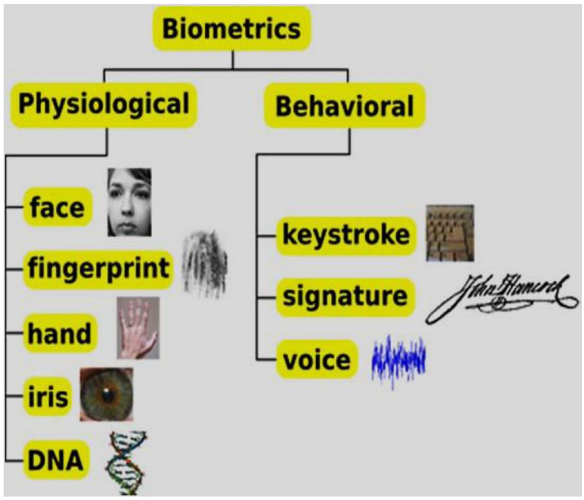

Figure1:Different Biometric Techniques

II. IRIS SCAN

Iris scanning may seem to be very ahead of the time, but core 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 ability to get acclimatized in any environment as an exceptionally accurate biometric is derived from

1. The difficulty of forging and by an imposter.
2. It's intrinsic isolation and protection from the external environment;
3. It's extremely data-rich physical structure.

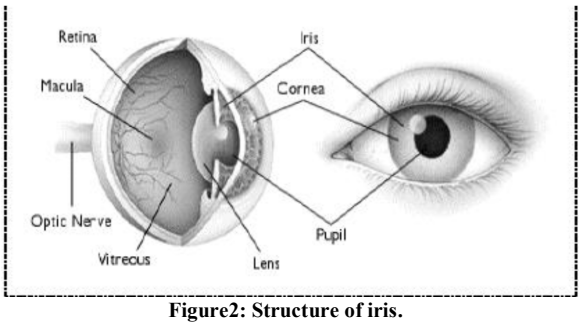

Figure2: Structure of iris.

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

v. It's 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. Since 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 imageenhancement. 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.

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

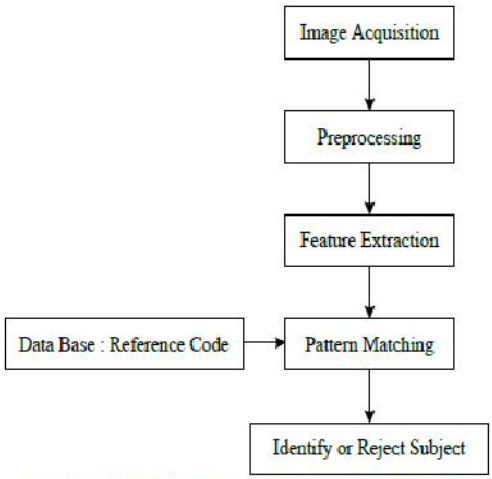

Figure 3: General steps of the iris recognition system

PREPROCESSING

(a)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.

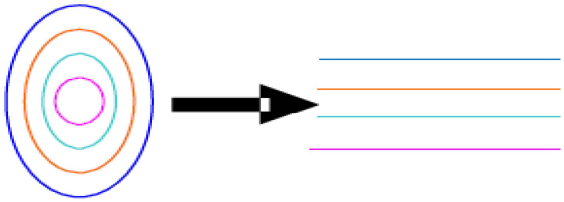

Figure 4: Polar transformation

(b) Correct iris segmentation:
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.

(c)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 *cosx0,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.

(d)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. Gaborand 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.

IV. METHODOLOGY

Security has become a serious issue in areas like airports banks, R&D deptetc 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.

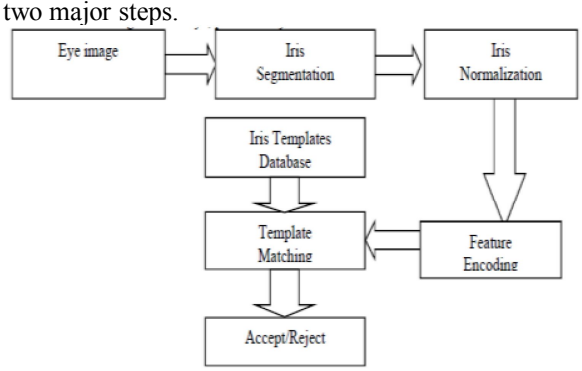

Fig 5: The Iris Recognition System

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, anddetection/removal of reflections from the cornea.

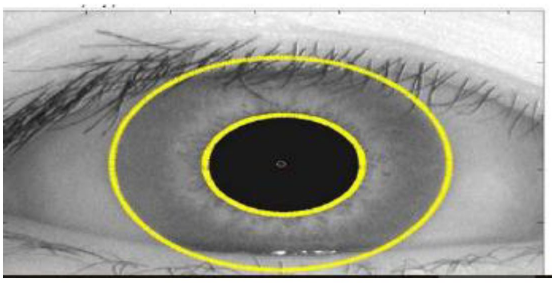

Fig 6: Iris Segmentation

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

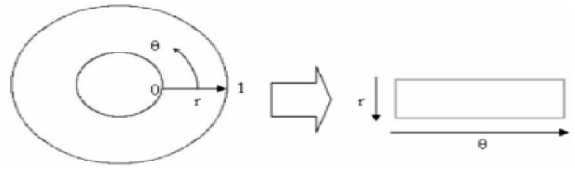

Fig 7: Iris Normalization

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:

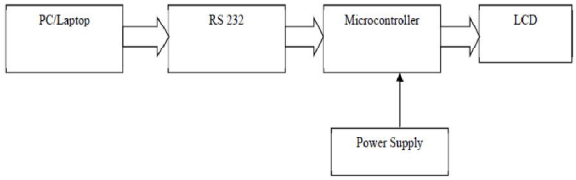

Fig 8: Block Diagram of Iris based security system using microcontroller

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

No contact required.

Protects internal organs

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 biometrics made it possible to verify this.

Disadvantages:

- .Difficult to capture for some individuals.
- Easily obscured by eyelashes, eyelids, lens and reflections from the cornea.
- 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] VanajaRoselin.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, csedeptmbescoe. ambajogai

[3] Harshadaterkhedkar 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] Induverma and sanjaykumarjain, "biometrics security system", ieee 2nd international conference on computing for sustainable global development, pp 1189-1192, 2015

★★★