ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 9, Issue 4, October 2019

Design & Implementation of Biometric Security System using Fingerprint & Iris Recognition

Shelar Nishigandha D, Lavate Prajakta, Gavale Prafulla

Abstract*— Biometric system plays important role in the security system. Authentication of the user with the use of the finger & Iris recognition system. The fingerprint module has the important with the thumb scanning with comparison with the database. If finger match then the system gives the full access if not permission denied. Iris based system used to store the Iris with the system with the comparison with the database. If match then it shoe the output on the LCD screen, if not matched then siren the buzzer. The processing of the Thumb scanner with the Microcontroller & Embedded C. The Iris processing is done in the MATLAB.

***Keyword*—Fingerprint, Iris, Security, Microcontroller.**

I. INTRODUCTION

In our project we are presenting the newly combined security system using the human organs called as biometric elements.

The most common biometric security systems use fingerprints, but these systems can also use iris and retinal scans, hand geometry, and facial recognition technology. Biometrics refers to metrics related to human characteristics.

A. Importance of Biometrics

Biometric is technique of using unique non transferable, physical characteristics, such as to gain entry for personal identification. It is a method of automatic verification of person based on some specific biometric features derived from her physiological and behavioral characteristics .However all these identification methods have weaknesses such as

- Face and iris can be recorded by camera.
- Speech can be recorded and replayed.
- Fingerprint can be recreated in lack using an object touched by that person.
- Signature can be reproduce easily.
- It is easy to steal a piece of DNA from an unsuspecting subject.

B. Introduction to basic biometric authentication

A new race of human being is drawing on the horizon. Which will be capable of acknowledging what some humans of today are preparing for them beyond traditional teachings, it no longer corresponds to the current era. In recent years, it has become very important to identify a user in applications such as personnel security, finance, airport, hospital and many other important areas [1].Human verification has traditionally been carried out by using a password and / or ID cards. To increase reliability and to reduce the, fraudulent use of identity a wide range of biometric is emerging e.g. fingerprint, face and iris.

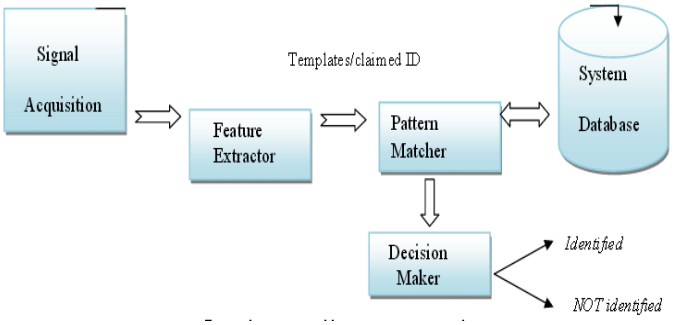


Fig1. Basic Diagram of Biometric Authentication

II. DESIGN OF BIOMETRIC SECURITY SYSTEM USING FINGERPRINT & IRIS RECOGNITION

Block Diagram Consist of

1)Thumb Scanner- Used to Take the fingerprint of the user & compare with the Stored data based .When Microcontroller provides the input it generate the output based on the match found or not found.

2) Iris scanner- Used to scan the retina of the human being. It is used to detect the Iris & send the Image to the PC for processing & the matching.

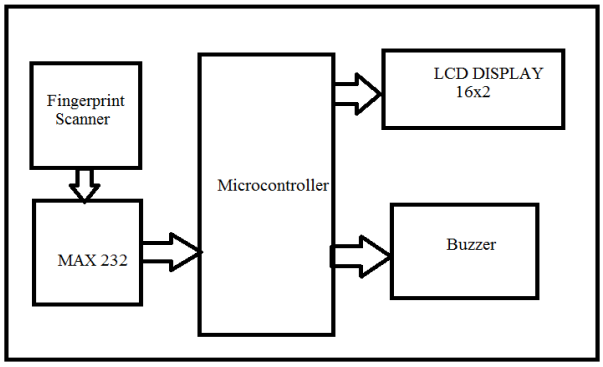
3) PC – It having the MATLAB software. It is used to read the input from the Iris scanner & generate the output according to it.

4) LCD- Used to display and generate the result on the screen & status of the all parameter values.

5) Buzzer- Siren the buzzer if the unauthorized entry detected.

6) UART 0 – It is used to interface the Thumb scanner with it.

7) Microcontroller– It is the main controller of the system. It is used to control all the parameters regarding as per the input from the Thumb & Iris scanner.



ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 9, Issue 4, October 2019

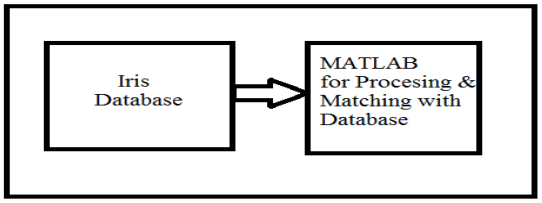


Fig 2. Block Diagram of System

III. WORKING

The P89V51RD2 is a low power, high performance CMOS 8 bit microcontroller with 4k bytes of flash programmable & erasable read only memory(PEROM).The device is manufactured using ATMELS high density non volatile memory technology &is compatible with the industries standard MCS-51 instruction set &pin out. The on-chip flash allows the program memory to be reprogrammed in system or a conventional non volatile memory programmer. By combining a versatile 8 bit CPU with flash on monolithic chip. The P89V51RD2 is a powerful microcontroller which provides a highly flexible & cost-effective solution to many embedded control applications.

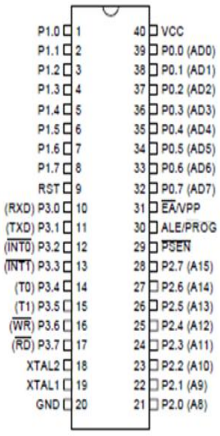


Fig 3. Microcontroller P89V51RD2

The main features of microcontroller are as follows.

1. Compatible with P89V51RD2
2. 64 kilobytes internal RAM.
3. Fully static operation 0Hz to 24MHz.
4.3 level program memory lock.
5.128x8-bit internal RAM.
6.32 programmable I/O lines.
7. Two 16 bit timer/counter.
8. Six interrupt sources.
9. Programmable Serial channel.
10. Full duplex serial port.

IV. FINGERPRINT SCANNER R303A SERIAL INTERFACE

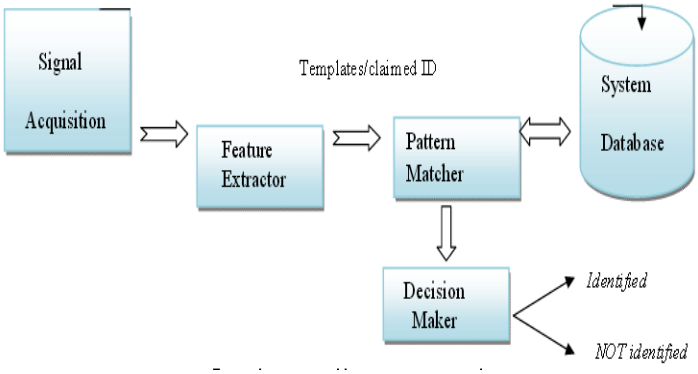


Fig. 4 Fingerprint Scanner R303a serial interface

A. FINGERPRINT MODULE

Fig.5 Fingerprint Module R303A

Specifications Fingerprint Module R303A

- Interface: USB 1.1 / UART (TTL logical level)
- Dimension: 56*20*21.5mm
- Image Capture Surface 14 x 18(mm)
- Verification Speed < 1 second
- Scanning Speed < 0.5 second
- Character file size: 256 bytes
- Template size: 512 bytes
- Storage capacity: 120/350/880
- Security level: 5(1, 2, 3, 4, 5(highest))
- False Acceptance Rate (FAR) < 0.001%
- False Rejection Rate (FRR) < 0.1%
- Resolution 500 dpi
- Voltage 3.6-6.0V DC via USB port

B. Working of Fingerprint Module

Actually thanks everyone for the help but I have accomplished what I wanted to do with my fingerprint module and finished my project 2 months ago. And someone has asked that how to generate and sore a char file, the procedure is right below

1. You have to read a finger image by using the byte stream:

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 9, Issue 4, October 2019

0xEF, 0x01, 0xFF, 0xFF, 0xFF, 0xFF, 0x01, 0x00, 0x03, 0x01, 0x00, 0x05

2. then after getting a success acknowledge you have to generate char file and store it in charbuff1 available in the module itself with a data packet mentioned in the R303A manual

3. then again read the finger image(always remember that a finger must be on the reader otherwise the module will return a negative acknowledge) and again generate a charfile and store in the charbuff2

4. now using the charfiles stored in charbuff1&2 you can create a template file(reduced fingerprint image) (Refer manual) which will be stored back in the character buffers back again then there is a command that is used to save the template file in the fingerprint library(flash memory available in the module) (very large).

There is also a command to search for finger template(acquired by the same procedure steps 1, 2, 3) which requires starting and end page addr of the search as parameters and returns a pageID(at which the matching template is present) in the acknowledge message.

Fig.6. Fingerprint Scanner Application

C. Advantages

The iris of the eye has been described as the ideal part of the human body for biometric identification for several reasons: It is an internal organ that is well protected against damage and wear by a highly transparent and sensitive membrane (the cornea). This distinguishes it from fingerprints, which can be difficult to recognize after years of certain types of manual labor. The iris is mostly flat, and its geometric configuration is only controlled by two complementary muscles (the sphincter pupillae and dilator pupillae) that control the diameter of the pupil. This makes the iris shape far more predictable than, for instance, that of the face. The iris has a fine texture that—like fingerprints—is determined randomly during embryonic gestation. Like the fingerprint, it is very hard (if not impossible) to prove that the iris is unique. However, there are so many factors that go into the formation of these textures (the iris and fingerprint) that the chance of false matches for either is extremely low. Even genetically identical individuals (and the left and right eyes of the same individual) have completely independent iris textures. An iris scan is similar to taking a photograph and can be performed from about 10 cm to a few meters away. There is no need for the person being identified to touch any equipment that has recently been touched by a stranger, thereby eliminating an objection that has been raised in some cultures against fingerprint scanners, where a finger has to touch a surface, or retinal scanning, where the eye must be brought very close to an eyepiece (like looking into a microscope). The commercially deployed iris-recognition algorithm, John Daugman's Iris Code, has an unprecedented false match rate (better than 10−11 if a Hamming distance threshold of 0.26 is used, meaning that up to 26% of the bits in two Iris Codes are allowed to disagree due to imaging noise, reflections, etc., while still declaring them to be a match).[13] While there are some medical and surgical procedures that can affect the color and overall shape of the iris, the fine texture remains remarkably stable over many decades. Some iris identifications have succeeded over a period of about 30 years. Iris recognition works with clear contact lenses, eyeglasses, and non-mirrored sunglasses.

D. Shortcomings

Many commercial iris scanners can be easily fooled by a high quality image of an iris or face in place of the real thing. The scanners are often tough to adjust and can become bothersome for multiple people of different heights to use in succession. The accuracy of scanners can be affected by changes in lighting. Iris scanners are significantly more expensive than some other forms of biometrics, as well as password and proximity card security systems. Iris scanning is a relatively new technology and is incompatible with the very substantial investment that the law enforcement and immigration authorities of some countries have already made into fingerprint recognition. Iris recognition is very difficult to perform at a distance larger than a few meters and if the person to be identified is not cooperating by holding the head still and looking into the camera. However, several academic institutions and biometric vendors are developing products that claim to be able to identify subjects at distances of up to 10 meters ("Standoff Iris" or "Iris at a Distance" as well as SRI International's "Iris on the Move" for persons walking at speeds up to 1 meter/sec). As with other photographic biometric technologies, iris recognition is susceptible to poor image quality, with associated failure to enroll rates. As with other identification infrastructure (national residents databases, ID cards, etc.), civil rights activists have voiced concerns that iris-recognition technology might help governments to track individuals beyond their will. Researchers have tricked iris scanners using images generated from digital codes of stored irises. Security considerations

As with most other biometric identification technology, a still not satisfactorily solved problem with iris recognition is the problem of live-tissue verification. The reliability of any biometric identification depends on ensuring that the signal acquired and compared has actually been recorded from a live

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 9, Issue 4, October 2019

body part of the person to be identified and is not a manufactured template. Many commercially available iris-recognition systems are easily fooled by presenting a high-quality photograph of a face instead of a real face, which makes such devices unsuitable for unsupervised applications, such as door access-control systems. The problem of live-tissue verification is less of a concern in supervised applications (e.g., immigration control), where a human operator supervises the process of taking the picture. Methods that have been suggested to provide some defence against the use of fake eyes and irises include changing ambient lighting during the identification (switching on a bright lamp), such that the pupillary reflex can be verified and the iris image be recorded at several different pupil diameters; analyzing the 2D spatial frequency spectrum of the iris image for the peaks caused by the printer dither patterns found on commercially available fake-iris contact lenses; analyzing the temporal frequency spectrum of the image for the peaks caused by computer displays.

Other methods include using spectral analysis instead of merely monochromatic cameras to distinguish iris tissue from other material; observing the characteristic natural movement of an eyeball (measuring nystagmus, tracking eye while text is read, etc.); testing for retinal retro reflection (red-eye effect) or for reflections from the eye's four optical surfaces (front and back of both cornea and lens) to verify their presence, position and shape. Another proposed method is to use 3D imaging (e.g., stereo cameras) to verify the position and shape of the iris relative to other eye features. A 2004 report by the German Federal Office for Information Security noted that none of the iris-recognition systems commercially available at the time implemented any live-tissue verification technology. Like any pattern-recognition technology, live-tissue verifiers will have their own false-reject probability and will therefore further reduce the overall probability that a legitimate user is accepted by the sensor.

E. Internal Details of Eye

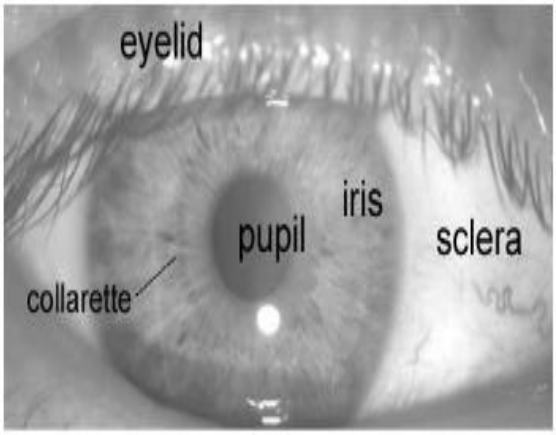


Fig.7. Internal Details of Eye

F. Eye Matching Process

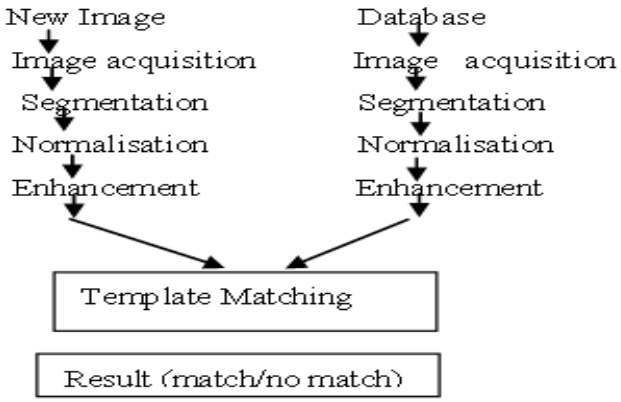


Fig. 8.Eye Matching Process

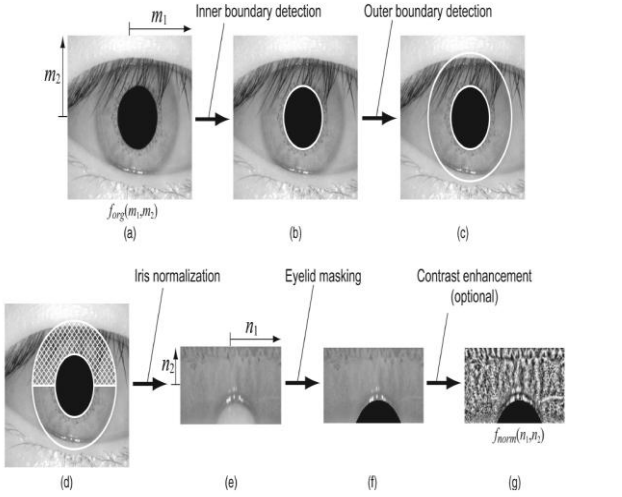


Fig. 3. Iris image preprocessing. (a) Original image $f_{org}(m_1, m_2)$. (b) Detected inner boundary. (c) Detected outer boundary. (d) Lower half of the iris region for matching. (e) Normalized image. (f) Normalized image with eyelid masking. (g) Enhanced image $f_{norm}(n_1, n_2)$.

Fig.9. Approach towards Eye matching

Abbreviation "e.g.," means "for example" (these abbreviations are not italicized).

An excellent style manual and source of information for science writers is [9].

V. ADVANTAGES

1) Highly Secure

2) No manual Intervention of Human being s to cite relevant prior work.

VI. APPLICATION

1) Bank Security System
2) ATM Access
3) Biometric Door Access
4) Attendance System

VII. CONCLUSION

A Microcontroller having the Serial Port. So by using the Serial port & Pins of TXD & RXD it is possible to interface the Fingerprint & the Iris module. Also it having the GPIO pins by using this LCD & Buzzer interface is easy part with respect to it. By using P89V51RD2 it fulfill the requirement

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 9, Issue 4, October 2019

of the system design. For the Iris reorganization MATLAB is suitable for matching the template with respect to it.

REFRENCES

[1] Kazuyuki Miyazawa, Koichi Ito" An Effective Approach for Iris Recognition Using Phase-Based Image Matching" IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 30, NO. 10, OCTOBER 2008.

[2] Jaishanker K. Pillai, Vishal M. Patel "Secure and Robust Iris Recognition Using Random Projections and Sparse Representations ", IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 33, NO. 9, SEPTEMBER 2011.

[3] Stefan Jenisch and Andreas Uhl, "SECURITY ANALYSIS OF A CANCELABLE IRIS RECOGNITION SYSTEM BASED ON BLOCK REMAPPING ", IEEE Conference on Image Processing 2011.