Access Control System Using Finger Print Biometric System

Abutu Silas
Department of Electrical and Electronic Engineering, Petroleum Training Institute, Effurun Delta State, Nigeria

Abstract: **Fingerprint identification is no longer the preserve of crime detection or science fiction. It's widely used in access control because it's a very reliable straightforward verification method unlike the traditional lock systems, passwords which were found not to secure perfectly. The major reason for this study is to provide an advance security for such high end security applications. The aim of this study is to design an access control system using finger print biometric system. This is to grant access only to authorized persons. An emergency alarm is incorporated to deter an intruder trying to gain access.**

***Keywords*- Fingerprint, biometrics authorized, intruder, Access, security, control.**

I. INTRODUCTION

Biometrics is the study of verifying the identity of a person through physiological estimations or social attributes. Since biometric identifiers are related forever with the user they are more dependable than token or information based validation strategies. Biometric layouts can't be figured out to reproduce individual data and they can't be taken and used to get to individual data.

Utilizing an exceptional, physical attribute of your body, for example, your fingerprint or iris, to easily recognize and confirm that you are who you guarantee to be, is the best and most effortless arrangement in the market today. That is the basic truth and intensity of Biometrics Technology today. Despite the fact that biometric innovation has been around for a long time, present day propels in this developing innovation, combined with enormous decreases in cost, presently make biometrics promptly accessible and moderate to buyers, entrepreneur, bigger organizations and public area offices the same.

A. Finger Print Uniqueness

A fingerprint is the pattern of ridges and valleys on the fingertip. The endpoints and crossing points of ridges are called minutiae. It is a generally acknowledged presumption that the minutiae pattern of each finger is one of a kind and doesn't change during one's life. Ridge endings are the focuses where the ridge curve ends, and bifurcations are the place a ridge parts from a solitary way to two ways at a Y-intersection. Fig. 1 shows a case of an edge finishing and a bifurcation. In this model, the dark pixels relate to the ridges, and the white pixels correspond to the valleys

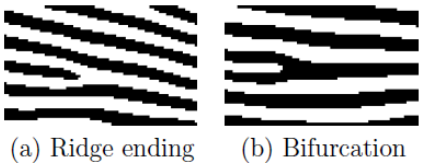

Fig.1: Example of a ridge ending and a bifurcation

How Does a Fingerprint Optical Scanner Work?

A fingerprint scanner system has two basic jobs -- it needs to get an image of your finger, and it needs to determine whether the pattern of ridges and valleys in this image matches the pattern of ridges and valleys in pre-scanned images.

Only specific characteristics, which are unique to every fingerprint, are filtered and saved as an encrypted biometric key or mathematical representation. No image of a fingerprint is ever saved, only a series of numbers (a binary code), which is used for verification. The algorithm cannot be reconverted to an image, so no one can duplicate your fingerprints.

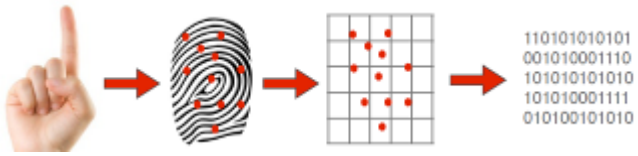

Fig. 2: Fingerprint optical scanner

Image source:

http://www.bioelectronix.com/what_is_biometrics.html

Advantages of Fingerprint

- It is highly accurate
- It is unique and can never be the same for two persons.
- It is the most economical technique.
- It is easy to use
- Use of small storage space

System Development Design

This system is centered on biometric traits of authorized users. The system design consists of hardware design and software design, implemented together to actualize a well secure access control. Figure 1 depicts the block diagram of the system. The system has several hardware components such as the Microcontroller, the Iris Scanner, the fingerprint Sensor, Keypad, LCD, Power Supply Unit and Door mechanism. The microcontroller PIC16f877A is an 8 bit microcontroller. The

fingerprint Scanner is used for the acquisition of an individual fingerprint image for use at the enrollment stage and also to confirm the authentication of individuals claimed identity. The fingerprint sensor has a self-adaptive adjustment mechanism that improves the quality of both dry and wet fingers, one of the advantages of this fingerprint sensor is the low cost and ease of use. The iris scanner is used to capture of iris image acquisition at enrollment and verification of identity. As a feedback to the user on operations of the system, a 16x2 LCD display is used. As an input device to the system, a multiplexed 4x4 matrix keypad is used to communicate with the device.

Overview of the System

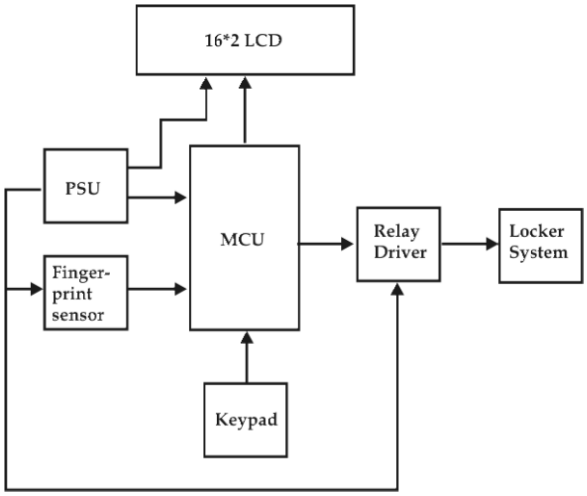

Fig. 3: Block Diagram of Access control system using fingerprint

A. *Enrolment Stage*

Every individual that wants to get authenticated to access what a biometric system protects must first of all enroll. The process involves the use of special scanners to acquire the fingerprint and iris of the user, creating templates of the images after segmenting, extracting the unique features and normalizing the images. Enrollment also gives room for the creation of profiles for users of the biometric system. The flowchart for the enrollment stage is shown in Figure 4. 3.4.

B. *Identification and Authentication Stage*

Once the individual has been enrolled into the system the user is then given access to the vault. Identification simple means a one to many matches requiring the user to provide either his fingerprint or his iris as a means of identification. The just acquired biometric sample presented for identification is compared to the previously stored sample in the database if there is a match with the fingerprint or iris pattern enrolled, access is provided to the vault door, and otherwise it is declined.

C. *The System's Database*

A database was created for the different users with the users' information after testing the functionality of the system with different users. The database contained the Admin passcode where after access, creation of users IDs was done with the acquisition of their passcode, their fingerprint and iris details which were later stored in the database for when authentication would be required.

II. SYSTEM DESIGN AND IMPLEMENTATION

A. *The Power Supply Unit*

This unit converts the 220V AC to 5V DC required by the circuit.

It was implemented with the following components:

- 220V/12V step down transformer
- Bridge Diode
- Capacitor
- Voltage regulator

Below is the circuit diagram of the power supply unit:

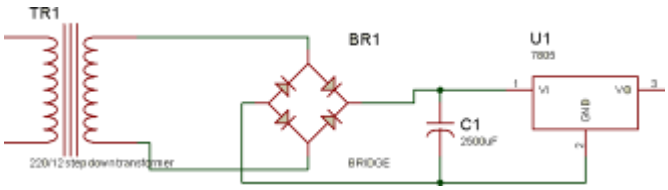

FIG 4 Power Supply Unit

Voltage regulator:

As we require a 5V we need LM7805 Voltage Regulator IC.

7805 IC Rating:

- Input voltage range 7V- 35V
- Current rating Ic = 1A
- Output voltage range Vmax = 5.2v; Vmin=4.8v

Transformer:

Selecting a suitable transformer is of great importance. The current rating and

The secondary voltage of the transformer is a crucial factor.

- The current rating of the transformer depends upon the current required for the load to be driven.
- The input voltage to the 7805 IC should be at least 2V greater than the required 2V output, therefore it requires an input voltage at least close to 7V.
- So I chose a 12-0-12 transformer with current rating 500mA (Since $12*\sqrt{2} = 16.97V$).

B. The Biometric Input Unit

This unit enables the system to capture the biometric print of the student/employees. It directly communicates with the microcontroller.

Requirements of the Biometric input Unit

- It should be able to effectively capture the biometric finger print of the user.
- It should have easy communication interface with a microcontroller
- It should have easy algorithm and have reasonable power requirements
- It should be available and cost effective

The SM630 Biometric finger print module was used to implement this unit.

Below are some of the basic features of the SM630 Module

Selection of the SM630 Biometric Finger Print Module

- It uses RS232 serial communication protocol at 9600 baud rate, which is easily adoptable by microcontrollers.
- It operates with 5V DC 0.15A
- It is well shaped and can be easily fitted.
- It assigns a unique ID for every captured Finger print
- It is readily available and cost effective.

Below is the circuit interface between the microcontroller and the SM630 Biometric finger print.

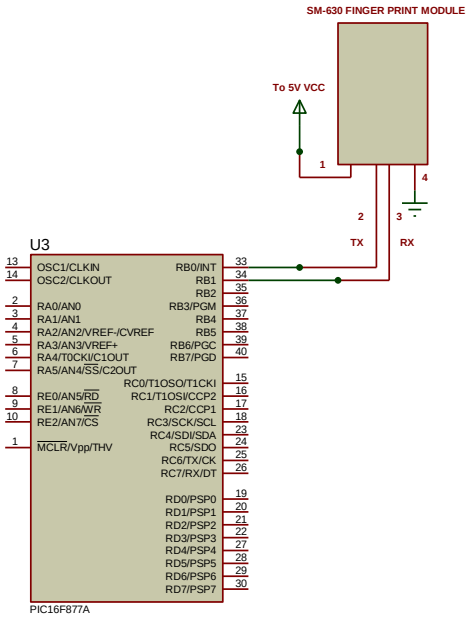

Fig: 5: Fingerprint Unit

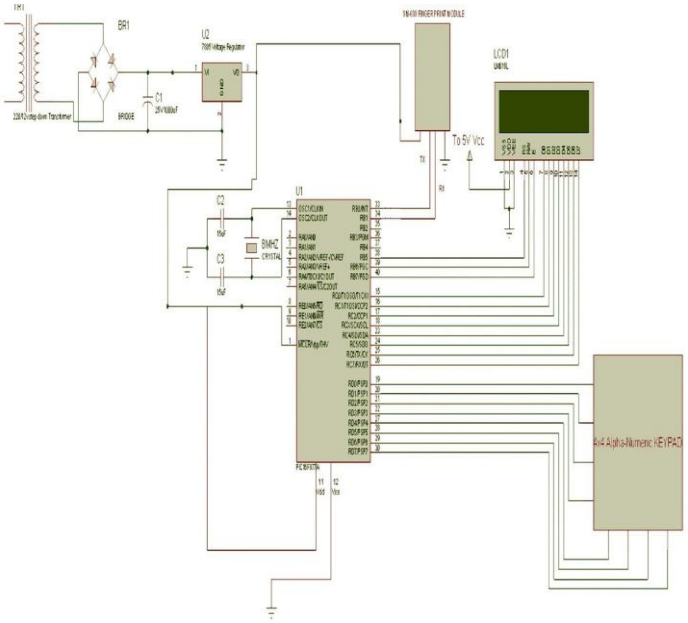

Fig. 6: system's operational diagram

III. SOFTWARE DESIGN

The programming language used in this project is C. The embedded C program implements the system flowchart. Simply put, it reads in binary patterns from the input subsystems and sends out binary patterns that would cause the required actions to be taken by the output subsystems

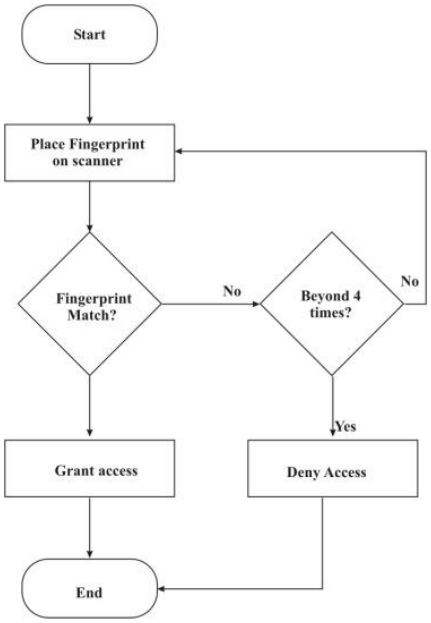

Fig. 7: Flow chart design of fingerprint access control

System Mode of Operation

The system work by coupling the designed model with the door lock to be controlled, and it should be placed in a way that user will be able to register their fingerprint into the

system database, the user does this by pressing the add new button on the keypad and to register the prints. When registered users places fingerprints on the device, the microcontroller sends a message to the relay unit which controls the opening of the door to grant access to the user, the door is closed manually by the user. If an unregistered user places his finger on the device, it will be denied access and if he continues, after three consecutive trials, the system will raise an alarm form the buzzer alert unit to notify the owner that an intruder is making an attempt to forcefully gain entrance to the secured area.

IV. RESULT

The implemented system was tested by collecting the fingerprints of some users and register them in the system database which makes them an authorized user of the system to test for the false rejection rate of the system, immediately the sensor scan their fingerprints, it grants access. The false acceptance rate was tested by asking the users that were registered in the database to place their finger on the sensor, to determine the accuracy and the confidentiality of the designed system.

False Acceptance Rate (FAR)

% FAR = FA/N x 100

Where

FA = No of incidence of false acceptance.

N = Total no of fingerprints sample in the database.

Having 10 users that has not been capture by the system and were allowed to try to gain access but 1 of them were granted access. Calculating the

%FAR = (1/10) x 100

= 10%

False Rejection Rate (FRR)

% FRR = FR/N x 100

Where

FR = No of incidence of false rejections

N = Total number of samples

Accessing by 20 registered users during testing it was discovered that 2 users were denied access. Calculating the %FRR

2/10 x 100 = 20%

Table 1: Testing Result

SN	Measure Quantity	% Value
1	FAR	10
2	FRR	20

The system responded according to the result shown in table 1, having a false acceptance of 20% and false rejection rate of 20%. The false rejection rate was observed to be due to some reasons like wet skin, injury on the fingertips, dry skin etc.

V. CONCLUSION

In this paper, an access control using fingerprint was developed to help control access of an unauthorized person to a facility or home. This system will help the user to maintain high level of security of life and properties thereby reducing the rate at which intruders access other people's belongings or asset.

ACKNOWLEDGMENT

Very big thanks to my HOD Engr. D.M Enweliku for his support and Also thank you to Engr. F.N. Nwukor, Engr Dr. T.O. Ayinde and the entire staff of Electrical and Electronic Engineering Department, Petroleum Training Institute, for their support towards the accomplishment of this research work.

REFERENCES

[1] Mittal, Yash & Varshney, Aishwary & Aggarwal, Prachi & Matani, Kapil & Mittal, Vinay. (2015). Fingerprint biometric based Access Control and Classroom Attendance Management System. 1-6. 10.1109/INDICON.2015.7443699.

[2] Umar, B.U, Olaniyi, O. M, Olorunyomi, J.A, (2016) Design And Development Of A Fingerprint Door Access Control System With A Buzzer Alarm, Proceedings of the International Conference on Science, Technology, Education, Arts, Management and Social Sciences (iSTEAMS Research Nexus).