ISSN 2349-7815

International Journal of Recent Research in Electrical and Electronics Engineering (IJRREEE)
Vol. 5, Issue 3, pp: (6-15), Month: July - September 2018, Available at: www.paperpublications.org

DEVELOPMENT AND EXPERIMENTATION OF A SECURITY DOOR LOCK SYSTEM USING BIOMETRIC FINGERPRINT ARCHITECTURE

[1]M. I. Efunbote, [2]M.B. Adeleke, [3]O. Fagbemi, [4]O. A. Orelaja, [5]R.A. Jokojeje

[1]Department of Electrical / Electronics Engineering, Moshood Abiola Polytechnic, Abeokuta, Ogun State, Nigeria
[2]Department of Mechanical Engineering, Moshood Abiola Polytechnic, Abeokuta, Ogun State, Nigeria

Abstract: **This research paper strictly focused on the use of a biometric fingerprint sensor in creating a security platform door lock. The system utilized a regulated 12v power supply from a 220volt alternative current , a relay control unit was incorporated which served as a switch in controlling the door lock system. A PIC168F77A microcontroller was connected to the transistor that regulated the relay control unit. The system was made up of a fingerprint sensor which sensed fingerprint input that was digitally interpreted and analyzed by a microcontroller unit. This microcontroller unit interpreted the input data fed into it by the fingerprint sensor and determined the opening and closing of the magnetic lock. This developed system performed as expected and the response time of the microcontroller unit was prompt, reliable, secured and accurate.**

Keywords: **Microcontroller, Magnetic Lock, Fingerprint Sensor, Relay Control Unit.**

1. INTRODUCTION

1.1 BACKGROUND OF STUDY:

There is high demand for the development of a low cost security system due to the recent security challenges in Nigeria in order to prevent terrorists, burglary and intruders from invading our homes. Several organizations are making attempt to secure, accurate identification, safe and reliable techniques to protect access to their services or operation. Biometric proffers solution to all these problems.

Biometrics deal with the analysis of the different parts of human body to get some specific features which will be used for identification purposes. The different parts of the body are thumbs, hands, faces, ears and others can be used in this technology. Biometrics offer a well- protected means of accessing sensitive areas and eliminate the necessity of carrying a card or trying to remember different types of passwords. In addition, this technology prevents stolen or issue of misplaced tokens. Different establishments are trying to get accurate, safe and proved techniques to protect means of accessing their services or operations. Biometrics is the solution to all these problems. The system is economical, easy to use andthe physical presence of the user is necessary for authentication purposes (MaltonMaio et al.,2003).Anil et al., 2004, Jain andPrabhakarn came up with a biometric recognition system that verifies and validates a person's identity by searching the database for match. Wang designed a pattern matching module that compares the extracted sectors with the stored templates which in turn generates matching score. Jea and Govindary 2005 use the flow network-based matching technique in fingerprint identification by decoding fingerprint image.Shimon et al.,2007 came up with a design that recognizes finger print detector for different age groups.Fingerprint recognition is widely used to identify individuals by looking at the different features presents in the users with a template which most people are used to.Nowadays, there are daily increments in crime rate all over the world. The bottom line is that all the previously invented security systems are highly customized, so in cases of failures or faults, they are not serviceable and repairable .It is mainly used for security purpose.

ISSN 2349-7815

International Journal of Recent Research in Electrical and Electronics Engineering (IJRREE)
Vol. 5, Issue 3, pp: (6-15), Month: July - September 2018, Available at: www.paperpublications.org

Matching Algorithm is the main technique used in this paper and a given template of fingerprints have been stored before. The fingerprints of the users are compared with the previously stored fingerprints in the templates. This technology confirms the fingerprints before the users can gain entrance into the door. Also, users may refuse to use some types of biometric identification due to possible hygiene misunderstandings, cultural differences and other exceptions due to their beliefs towards biometrics fingerprint recognition. Fingerprint recognition is mainly used today in places such as Banks (for ATMs), Schools (at the entrance of an examination hall), Airports, Governments, the legal system and other organizations. It is built into devices such as laptops.This system provides a security system to an office, the fingerprint sensor notices the thumb impression of the corresponding person and that image is compared with the registered image, if the two matches each other, the fingerprint device sent signal to the door, the door to the office will be activated immediately without anybody's assistance. This design is divided into two parts, the first one is master or controller mode and the second is user mode. The controller stores the new user mode in an ordinary mode used for the authentication and verification (permission) of the user. In the user mode of the point of authorization, the addition and removal of a user cannot be done. The permission of anybody registered on the master mode is recorded by adding the real time and date on to the biometric fingerprint with the use of real time module, data and time are recorded and stored in an SD for references. The biometric or fingerprint authentication based identification is most efficient and reliable solution for strength security.This study provides a serviceable and repairable sytem.The objectives of this work is to develop a software that controls an hardware automatically using C language and create a real time security system that opens and closes door automatically.

2. ARCHITECTURE OF PIC-BASED DOOR LOCK SYSTEM

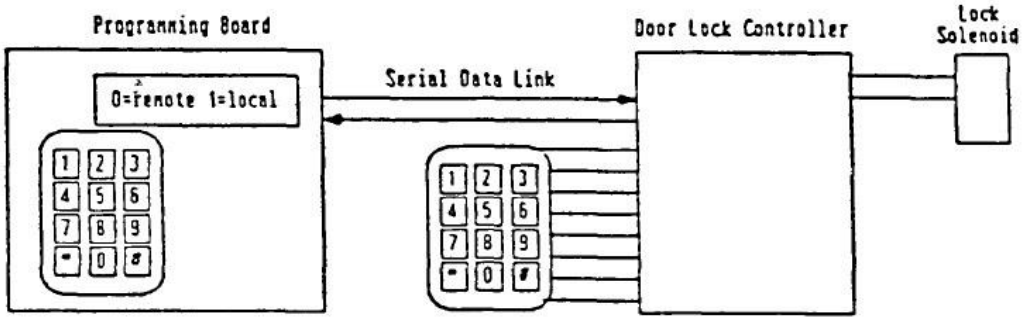

Figure 1: Showing system diagrams of door lock controller and programming modules

The Microprocessor-controlled door lock system done by Poirier and Vishnubhotla, 1990, pointed out that maintaining an entry only to authorized persons for multi-dwelling buildings such as apartments, dormitories, etc. is a problem. The system is composed of two modules, the door lock controller board and the programming board shown in Figure 1.

Based on these studies, researchers learned that microcontrollers can also be used for locking and unlocking doors for better safety and security.

2.1 HARDWARE DEVELOPMENT BLOCK DIAGRAM:

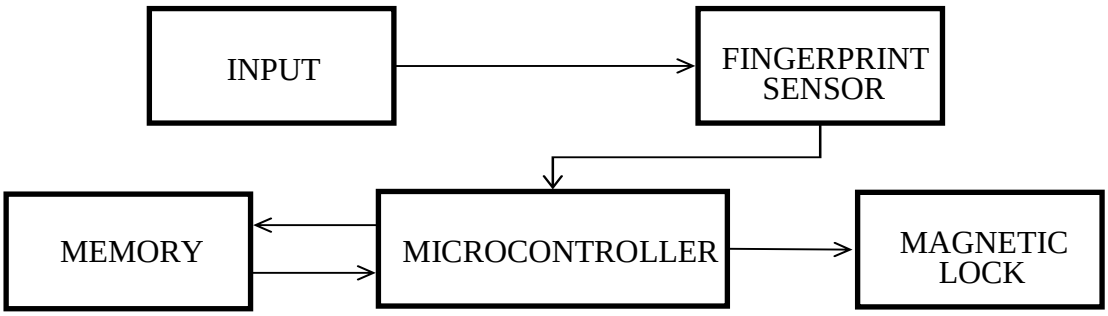

Figure 2: Block Diagram of the Design

The block diagram serving as the backbone of the design and figure 3-1 illustrates the circuit diagram used for the project.

ISSN 2349-7815

International Journal of Recent Research in Electrical and Electronics Engineering (IJRREEE)
Vol. 5, Issue 3, pp: (6-15), Month: July - September 2018, Available at: www.paperpublications.org

3. DESIGN ANALYSIS

Figure 3 shows the circuit diagram of the USB Door Lock using Biometrics Fingerprint Technology. The schematic diagram is divided into three units which are the USB Door Lock, Relay, and the Fingerprint Reading Device. The USB Door Lock system is the main system that is placed in the door and needs the Fingerprint Reading Device to be activated. The USB Door Lock system will be regulated from 220V AC to 12V to be able to work effectively with the operating state of the PIC168F77A microcontroller unit. The operating state of the microcontroller is referenced from its datasheet. A 470 micro-Farad capacitor is connected to the output voltage of the regulator and the ground to filter out the noise coming from the regulator. The relay driver circuit controlled the AC power used by the USB Door Lock system which consists of a PNP-transistor, 22 kilo-Ω resistor, 12V relay and 1N4006 diode. The 22kilo-Ω resistor allows small current to pass through the base-emitter junction. The output lines of the relay circuit are then connected to the output port RC5 of PIC168F77A, and to the 1N4006 diode and is connected to the 12V output of the regulator of door lock system and lastly it is connected to the ground. The transistor serves as a circuit that controls the state of the relay. When a small positive volt (3.3V) was applied at the base of the transistor, the collector-emitter junction connects together. Thus, the 12V power flows through the inductor part of the relay which then energizes the switch inside the relay. The state of the switch determines if the AC power flow to the AC socket. The reverse-biased diode serves as a voltage protection for the inductor part of the relay such that no current will pass through when the transistor is not active. If ever no positive voltage is applied to the base of the transistor, the transistor will not be in active state and the AC power is disconnected to the AC socket. The fingerprint reading device is the one responsible for collecting user's fingerprints. It is regulated by a 5V output voltage. An oscillator of 20 MHz is connected to one of the microcontroller's pin for the purpose of timing frequency.

The formula used in getting the value of the capacitor in the relay circuit is:

$$C=\frac{5I}{VF}=\frac{5\times7.59\times10^{-4}}{5.7\times20\times10^{6}}=33.29p^{f} \text{ equation } \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\text{...(1)}$$

Where:

C= computed capacitance in farads (F),

I = measured output current from the supply in amps (A),

V = measured supply voltage in volts (V),

f = frequency of the AC supply in hertz (Hz)

The base resistor of each transistor circuit is obtained using the formula:

$$R_b=\frac{V_b-V_{be}}{I_b}=\frac{5.7-0.7}{2.27\times10^{-4}}=22.02\text{k}\Omega$$

Where:

R_b = computed base resistor in ohms

V_b = the base voltage in volts (V)

V_{be} = the difference from the base voltage to the base emitter

I_b = measured base current in amperes (A)

3.1 SCHEMATIC DIAGRAM:

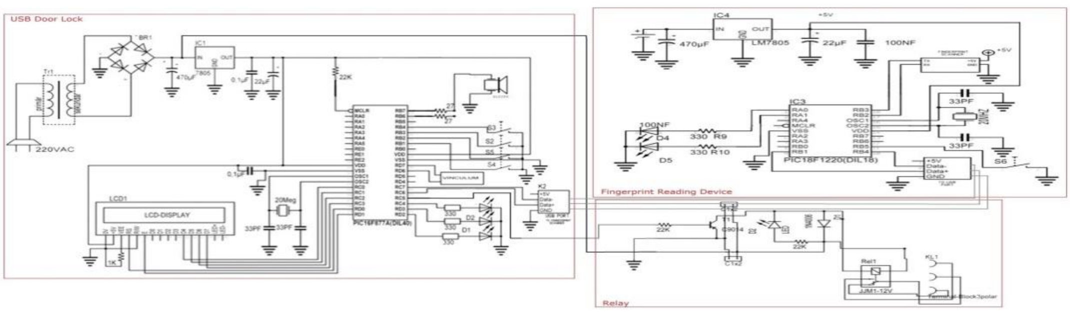

Figure 3: Schematic Diagram – USB Door Lock using Biometrics Fingerprint Technology

ISSN 2349-7815

International Journal of Recent Research in Electrical and Electronics Engineering (IJRREEE)
Vol. 5, Issue 3, pp: (6-15), Month: July - September 2018, Available at: www.paperpublications.org

3.2 SOFTWARE DEVELOPMENT PROGRAM FLOW CHART:

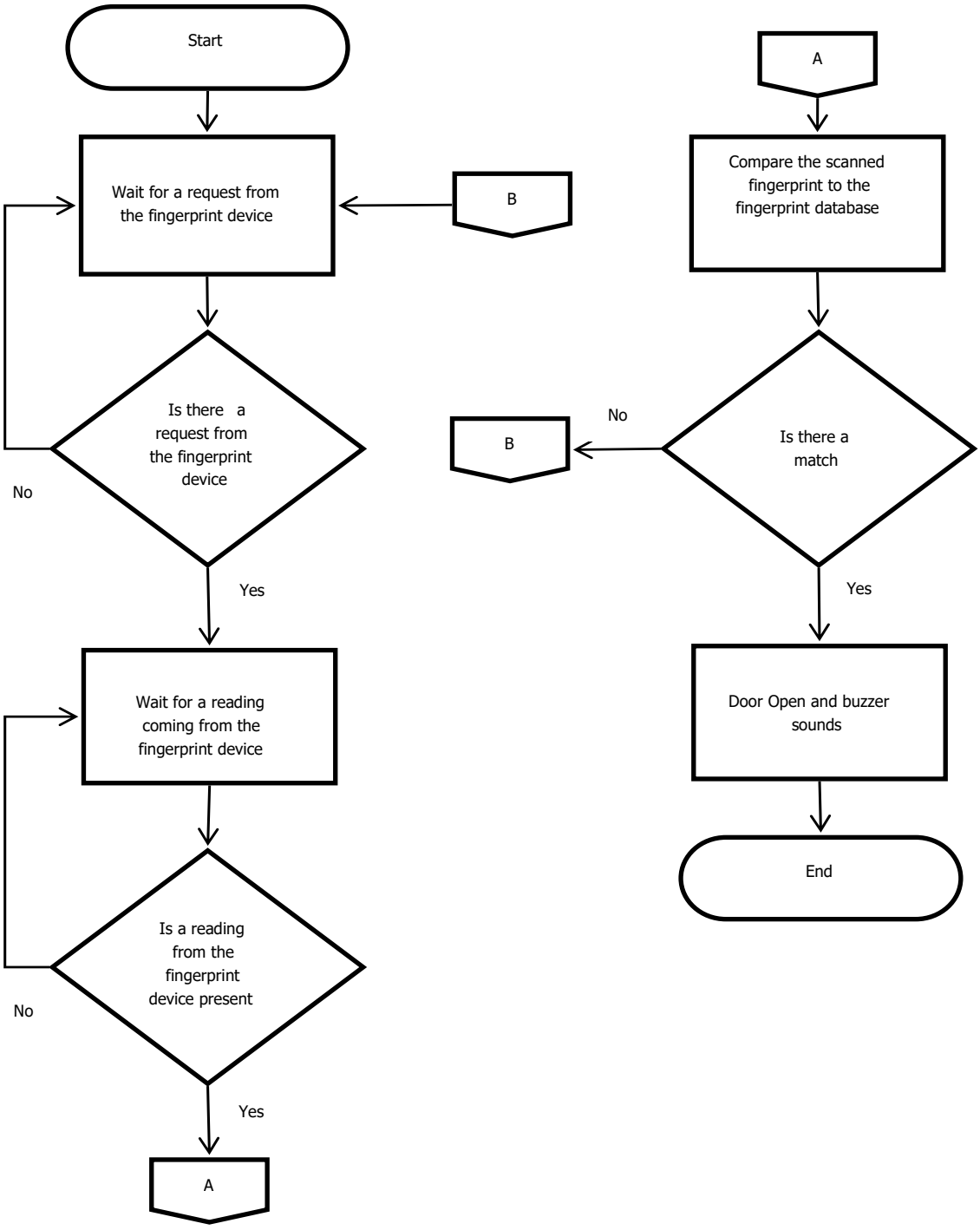

Figure 4: Door Access Flow Chart of Enrolled and Not enrolled users

ISSN 2349-7815

International Journal of Recent Research in Electrical and Electronics Engineering (IJRREEE)
Vol. 5, Issue 3, pp: (6-15), Month: July - September 2018, Available at: www.paperpublications.org

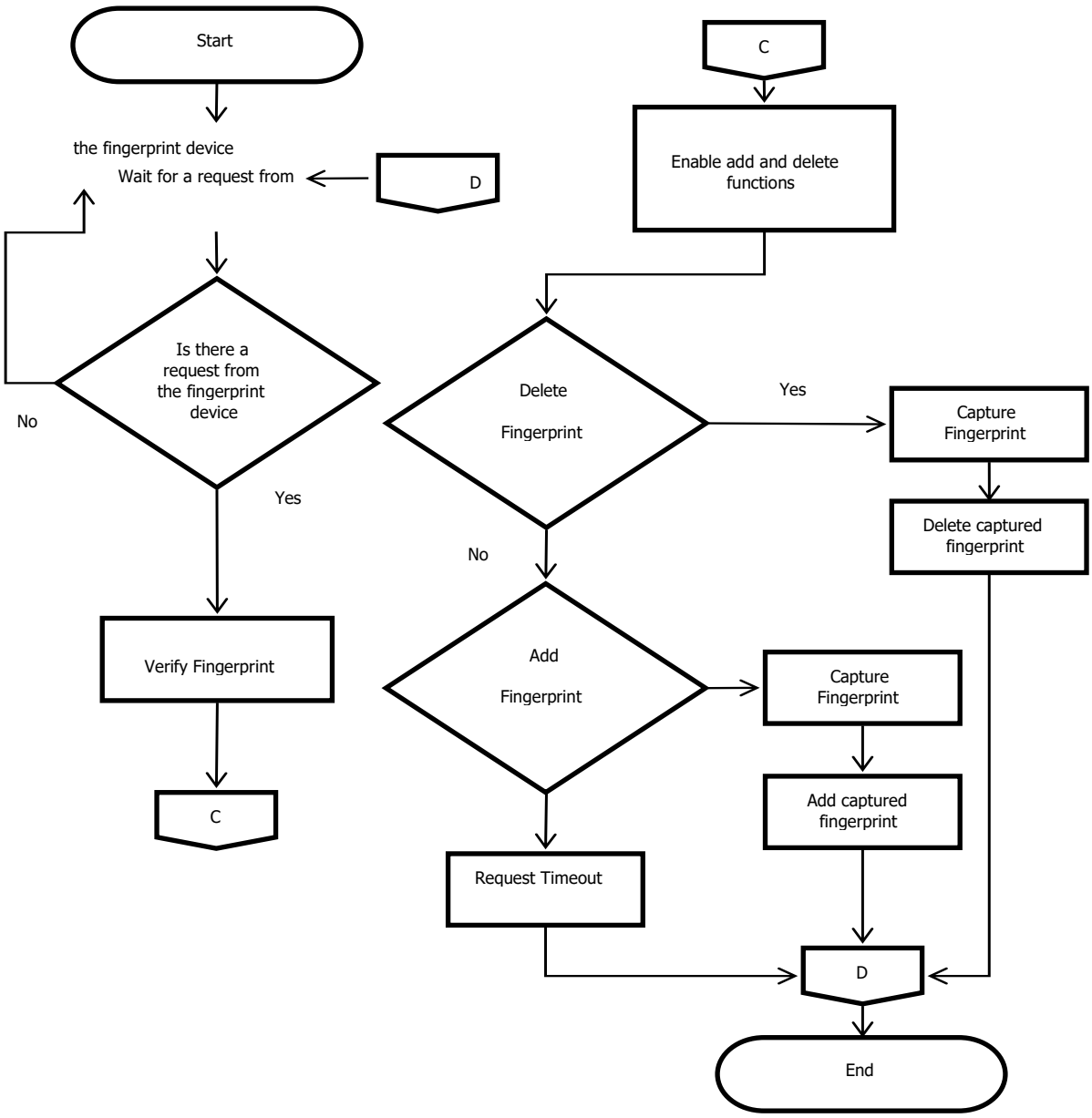

Figure 5: Door Access Flow with Administrator Rights

The following figures, referring to figure 4 and figure 5, are the flow charts of the prototype being design. It shows the processes of the verification and enrolment features of the USB Door Lock System using Biometrics Fingerprint Technology. The system starts up as soon as it is plugged in and automatically initializes all the variables needed to clear unwanted data that may cause system failure. The system awaits the request from the fingerprint reading device before any actions can be taking, in which authentication of fingerprint is always the first thing to do. Whether the user wants to open the door or enroll a new fingerprint, the system will always verify first, if the requesting user's fingerprint is registered. Unlocking the door just requires the microcontroller to verify the user and as soon as the system recognizes that the requesting user's fingerprint is registered, the door lock will open, immediately sound the buzzer prompting that it is opened for attacks and must be closed to activate the locking system again. The enroll feature happens only when the user is inside the room or establishment, assuming the requesting user's fingerprint is indeed stored in the system. After verification of the user's fingerprint, the system will prompt that the user is logged in and the enroll feature is enabled. When the enrolment is done, it will again verify the fingerprint to be enrolled by capturing three samples of the fingerprint and add it into the system prompting the fingerprint number for both the door lock system and the controller.

ISSN 2349-7815

International Journal of Recent Research in Electrical and Electronics Engineering (IJRREEE)
Vol. 5, Issue 3, pp: (6-15), Month: July - September 2018, Available at: www.paperpublications.org

4. TESTING AND RESULT ANALYSIS

4.1 TESTING:

The circuit diagram was simulated to ascertain its workability with the use of proteus software, the components were first tested by connecting them together on the breadboard following the circuit diagram to ensure that the circuit was okay. After this, it was transferred to the Vero-board for soldering. The construction of each unit was carefully done and tested. The construction started from the power supply unit, fingerprint sensor, microcontroller and finally connection of the magnetic door lock.

4.2 RESULT ANALYSIS:

The system verified whether the scanned fingerprint was enrolled or not, it add and delete fingerprint functions for registered fingerprints.

Procedure for the verification feature:

The system was plugged and made sure it was functioning properly without errors seen in the LCD.

1. Turn on the fingerprint reading device.
2. Insert the device into the system.
3. Push the verify button and wait for the fingerprint scanner to light up.
4. Once the scanner lights up, scan the fingerprint and wait if the door opens or not.
5. Repeat step 3 every time a user access the door lock.

Procedure for the enrollment features:

1. Firstly, plug the system and make sure it is functioning properly without errors seen in the LCD.
2. Turn on the fingerprint reading device.
3. Make sure you are inside the room or establishment then insert the device into the system.
4. Push the verify button in the system and in the device, respectively, and wait for the fingerprint scanner to light up.
5. Once the scanner lights up scan the fingerprint and wait if the LCD indicates that the user is logged in.
6. Push the add button and wait until the device lights up.
7. Scan the new fingerprint thrice and wait until the LCD indicates the fingerprint number for both the system and the fingerprint reading device.
8. Repeat step 3 every time new a user or fingerprint is to be enrolled.

The following tables illustrate how the features of the USB Door Lock System were tested to ensure all functionalities were working properly.

Table 1: Verification and Unlocking

TRIAL	VERIFICATION	STATUS
1	VERIFIED	UNLOCKED
2	VERIFIED	UNLOCKED
3	VERIFIED	UNLOCKED
4	VERIFIED	UNLOCKED
5	VERIFIED	UNLOCKED

6	VERIFIED	UNLOCKED
7	VERIFIED	UNLOCKED
8	VERIFIED	UNLOCKED
9	NOT VERIFIED	LOCKED
10	NOT VERIFIED	LOCKED
11	NOT VERIFIED	LOCKED
12	VERIFIED	UNLOCKED
13	VERIFIED	UNLOCKED
14	VERIFIED	UNLOCKED
15	VERIFIED	UNLOCKED
16	VERIFIED	UNLOCKED
17	VERIFIED	UNLOCKED
18	VERIFIED	UNLOCKED
19	VERIFIED	UNLOCKED
20	NOT VERIFIED	LOCKED
21	NOT VERIFIED	LOCKED
22	VERIFIED	UNLOCKED
23	VERIFIED	UNLOCKED
24	VERIFIED	UNLOCKED
25	VERIFIED	UNLOCKED
26	NOT VERIFIED	LOCKED
27	VERIFIED	UNLOCKED
28	VERIFIED	UNLOCKED
29	VERIFIED	UNLOCKED
30	VERIFIED	UNLOCKED

Based on the results, the USB Door Lock System designed prototype accurately verified if the captured or scanned fingerprint is enrolled or not in the database. There were some instances that even if the finger was enrolled, the system would not unlock the door since the verification depended on how that specific finger was scanned during its enrollment to the system as the fingerprint reading gathers three samples of scanned fingerprint template for accuracy.

Table 2: Enrolling and Locking

TRIAL	VERIFICATION	STATUS
1	NOT ENROLLED	LOCKED

2	NOT ENROLLED	LOCKED
3	NOT ENROLLED	LOCKED
4	NOT ENROLLED	LOCKED
5	NOT ENROLLED	LOCKED
6	NOT ENROLLED	LOCKED
7	NOT ENROLLED	LOCKED
8	NOT ENROLLED	LOCKED
9	NOT ENROLLED	LOCKED
10	NOT ENROLLED	LOCKED
11	NOT ENROLLED	LOCKED
12	NOT ENROLLED	LOCKED
13	NOT ENROLLED	LOCKED
14	NOT ENROLLED	LOCKED
15	NOT ENROLLED	LOCKED
16	NOT ENROLLED	LOCKED
17	NOT ENROLLED	LOCKED
18	NOT ENROLLED	LOCKED
19	NOT ENROLLED	LOCKED
20	NOT ENROLLED	LOCKED
21	NOT ENROLLED	LOCKED
22	NOT ENROLLED	LOCKED
23	NOT ENROLLED	LOCKED
24	NOT ENROLLED	LOCKED
25	NOT ENROLLED	LOCKED
26	NOT VERIFIED	LOCKED
27	NOT VERIFIED	LOCKED
28	NOT VERIFIED	LOCKED
29	NOT VERIFIED	LOCKED
30	NOT VERIFIED	LOCKED

Table 2 Verify Not Enrolled Fingerprint

Based on the results for the verification of not enrolled fingerprints, the USB door lock system designed prototype accurately verified that the captured or scanned fingerprint was not in the memory or enrolled into the system. This proved that the design could secure places where it will be installed with 100% accuracy in verifying intruders or untrusted access.

ISSN 2349-7815

International Journal of Recent Research in Electrical and Electronics Engineering (IJRREEE)
Vol. 5, Issue 3, pp: (6-15), Month: July - September 2018, Available at: www.paperpublications.org

Table 3: Template addition and Enrolling

TRIAL	MODE	STATUS
1	ADD TEMPLATE	ENROLLED
2	ADD TEMPLATE	ENROLLED
3	ADD TEMPLATE	ENROLLED
4	ADD TEMPLATE	ENROLLED
5	ADD TEMPLATE	ENROLLED
6	ADD TEMPLATE	ENROLLED
7	ADD TEMPLATE	ENROLLED
8	ADD TEMPLATE	ENROLLED
9	ADD TEMPLATE	ENROLLED
10	ADD TEMPLATE	ENROLLED
11	ADD TEMPLATE	ENROLLED
12	ADD TEMPLATE	ENROLLED
13	ADD TEMPLATE	ENROLLED
14	ADD TEMPLATE	ENROLLED
15	ADD TEMPLATE	ENROLLED
16	ADD TEMPLATE	ENROLLED
17	ADD TEMPLATE	ENROLLED
18	ADD TEMPLATE	ENROLLED
19	ADD TEMPLATE	ENROLLED
20	ADD TEMPLATE	ENROLLED
21	ADD TEMPLATE	ENROLLED
22	ADD TEMPLATE	ENROLLED
23	ADD TEMPLATE	ENROLLED
24	ADD TEMPLATE	ENROLLED
25	ADD TEMPLATE	ENROLLED
26	ADD TEMPLATE	ENROLLED
27	ADD TEMPLATE	ENROLLED
28	ADD TEMPLATE	ENROLLED
29	ADD TEMPLATE	ENROLLED
30	ADD TEMPLATE	ENROLLED

Table 4 Enroll New Fingerprint

Based on the gathered data for enrolling a new fingerprint template into the system, new fingerprints can be accurately enrolled into the system given that the user has administrative rights the user's fingerprint is already enrolled where testing results for verifying enrolled fingerprints were shown in Table 1.

5. CONCLUSION

There are various existing door locks using biometric fingerprint technology and most of them combined the fingerprint device into the door lock itself. The expected results were obtained from the integration of the fingerprint reader and a microcontroller using USB as its main connection. This design also proved that it could improve the level of security of establishments using the mechanical door locks through each person's fingerprint. The testing process showed that the system could correctly identify and compare fingerprint templates at a high rate whether it was to enroll a new fingerprint template or just verify if the captured template was in the memory or already enrolled. By means of this design, people will have an easier way of having a comfortable, secured, and authorized entrance in a certain building or establishment as there would be no keys, passwords or cards will be used. Users would register trusted fingerprints that could enter its premises. With this system, it could activate door locks and help people especially security guards, administrators and owners to secure its premises.

This design has offered a repairable and serviceable system.

REFERENCES

[1] Anil K. Jain, Arun Ross, SalilPrabhakur. "An introduction to Biometric Recognition" Volume 14(1), Pages 1-17, 2003.

[2] Anil K. Jain, Sharath P, Salil P, Lin Hong, Arun Ross. "Biometric: A grand challenge" Volume 2, Proceedings of Conference on Pattern Recorgnition,Cambridge,U.K,Pages 935-942,2004.

[3] Guodong Li, Hu Chen; "A new high level security portable system based on USB key with fingerprint, Computer Design and Applications Conference,China,25-27 June, 2003

[4] Jea T.Y and Govindary V " A minute-biased partial fingerprint recognition system. Volume 38.

[5] Poirier D.C,Vishnubhotla A . "A microprocessor-controlled door lock system" IEEE Transactions on consumer Electronics 36(2),Pages 129-136,1990.

[6] Prabhakar S, Pankanti S; Jain AK "Biometric recognition; Security and privacy concerns" Volume 99(2), Pages 33-42,2003.

[7] MaltoniD,MaioD,Jan,A.K and Prahbhakar .S "Handbook on Fingerprint Recognition"Springer,NewYork,Pages 57-85 ,2003.

[8] Shimon K. Modi, Stephen J. Elliott, Hakil Kim, "Impact of age groups on Fingerprint Recognition performance", 7-8 June 2007.

[9] Wang N.J and K.N Platinus "An analysis of random projection for changeable and privacy preserving Biometrics verification". IEEE Transactors on systems MAN and cybernetics- PART B CYBERTETICS Volume 40(5),2010.