

Design and implementation of Microcontroller-Based File Cabinet Security System using C-language

¹Ufoaroh S.U., ²Okonkwo R.O., ³Ezeagwu C.O ⁴Erike U.C

^{1,3,4}Department of Electronic and Computer Engineering, Nnamdi Azikiwe University, Awka, Nigeria.

²Department of Computer science, Nnamdi Azikiwe University, Awka, Nigeria

¹sufoaroh@yahoo.com,

²oobi2971@yahoo.com

³ogwugwuamezeagwu@gmail.com

⁴linora93@yahoo.com,

Abstract- Biometric technologies are becoming the foundation of an extensively array of highly secure identification and personal verification solutions. It is an automated method of recognizing an individual based on physiological characteristics such as fingerprints. This work is a fingerprint based biometric cabinet lock that uses individual fingerprints for verification and authentication for a secure access to the cabinet. It is a microcontroller based lock that uses a correct fingerprint pattern as a password to unlock the door of the cabinet. An electromagnetic solenoid lock was used in this project to perform the locking mechanism. An Arduino Uno is used as the controller of the electronic locking mechanism, the system was simulated using proteus software, the program code was written in C language using an Arduino IDE after which it was uploaded into the microcontroller. A fingerprint module (SM630) is used to provide the user with an input peripheral on which finger is placed.. A liquid crystal display (LCD) is used as a platform for the system to exhibit its conditions and status as well as to allow the user to select the desired menu option. During authentication, the user's fingerprint is scanned, upon successful authentication, the electronic lock unlocks and the user will be allowed to access the cabinet. On the other hand if the scanned fingerprint does not match any in the stored database, the electronic lock remains locked and access is denied, it will be displayed on the LCD and the cabinet will remains locked.

Keywords: unique authentication, biometric security, file cabinet locker, fingerprint module, Arduino Uno.

1.0 Introduction

Biometric identification for security systems has proven itself to be the most trustworthy and efficient form of security pass authentication. This work seeks to present a method of file cabinet security in which methods of access is wholly unique to the authorized individual through personal biometric identification in the form of a fingerprint. The works involves having an office file cabinet that uses a person's fingerprint as a form of security to control its lock in order to prevent an unauthorized access to the cabinet's contents (documents and valuables). A fingerprint module reads the fingerprint, searches for a match in a stored fingerprint database and once a match is found allows access to the cabinet's contents by opening the lock. By designing and constructing a biometric fingerprint based cabinet locking system, the problems common among other kinds of locking mechanism would be solved.

fingerprint based cabinet lock system which provides security for an office cabinet.

An office cabinet is used to store important or confidential files and other important documents, items and office equipment for the purposes that for any person(s) with jurisdiction over the items stored, wouldn't find any of the files or items missing as a result of theft.

The keypad lock, security cards and lately the high technology biometrics are the various ways for making an office cabinet secure.

Biometrics are automatic methods for identifying a person on the basis of some biological or behavioral characteristics [1].

Human beings have used fingerprints for personal identification for centuries, and they have used them for criminal investigations for more than 100 years. The validity of fingerprints as a basis for personal identification is thus well established.

and the patterns of any one individual remain unchanged throughout life. Fingerprints are so distinct that even the prints of identical twins are different. The prints on each finger of the same person are also different [2].

The level of detail in fingerprint images scanned into a biometric system depends on several factors. They include the amount of pressure applied to the fingertip during image scanning, the presence of any cuts or other deformities on the fingertip, and the dryness of the skin. Therefore, any unusual or prominent features on a fingertip, the endings of the fingerprint ridges, and ridge bifurcations, or branches—collectively known as minutiae—are all used in a biometric system based on fingerprint identification.

The development of solid-state modules for fingerprint scanning may soon make the cost of incorporating a fingerprint-based biometric device affordable in many applications, such as laptop computers and cellular telephones. Consequently, researchers expect fingerprint identification to be the leading biometric technique in the near future [3].

Biometric identification for security systems has proven itself to be most trustworthy and efficient form of security pass authentication. This work seeks to present a method of file cabinet security in which methods of access is wholly unique to the authorized individual through personal biometric identification in the form of a fingerprint. The work involves having an office file cabinet that uses a person's fingerprint as a form of security to control its lock in order to prevent an unauthorized access to the cabinet contents (documents and valuables). A fingerprint module reads the fingerprint, searches for a match in a stored fingerprint database and once a match is found allows access to the cabinet's contents by opening the lock. By designing and constructing a biometric fingerprint based cabinet locking system, the problems common among other kinds of locking mechanism would be solved.

2.0 Review of Related Works

So many works have been done by researchers in the area of biometric security system in recent times.

In the work of [4], the microcontroller Atmel 8051 was used to control the scanning process of the fingerprint, after verification, a password is

entered to open the locker through a keypad, this work is a combination of both biometric fingerprint and keypad pin verification which works well in providing a double layer security which is very good, but the extra security pin verification is redundant for an office file cabinet.

In the work of [5] in which fingerprints are identified by mobile devices using only a person's finger and then afterwards, the device is connected to an office computer database for verification. Such work risks software incompatibilities whereby the device might come with windows XP whereas the designed fingerprint application runs on windows 7. In the same work [5], the fingerprint module used requires drivers to which they might not have a source code and if the Operating system (OS) platform changes, that might also become a risk. A common characteristic in the two works reviewed above is that they both use fingerprint biometrics to control the locking system. A different kind of biometrics could be used in security verification, as seen in the work of [6] where speech recognition in a tiny mega32 microcontroller in which real time speech processing was used to control a system that will unlock upon recognizing a voice password spoken by the administrator. This work was made possible by the implementation of band pass filters in the assembly language with fixed point format onto the microcontroller.

The problem of software incompatibility in the work of [5] is solved in this paper, as the Integrated Development Environment (IDE) used in developing the code is compatible with all versions of window. Also the challenge of inconsistent source code for fingerprint sensor drivers as experienced in the same [5] work is solved by the use of a modern fingerprint module which uses serial communication for transferring data and commands between it and the microcontroller thereby eliminating the need for drivers. This paper is aimed at presenting a fingerprint based authentication Biometric cabinet lock, that is low cost, compact in size and standalone system.

3.0 System Designs

The methodology adopted for the design of this work involves the integration and interfacing of the various sub units of the work together. The block design is shown in Fig. 1.

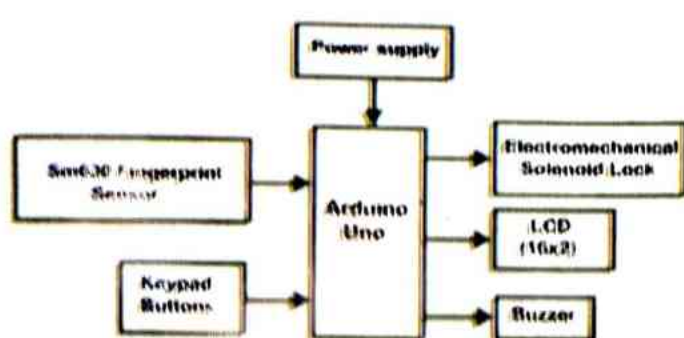


Fig.1: Block Diagram of Biometric File Cabinet Security System

The Functional Units of the system include:

A. SM630 Fingerprint Module.

SM630 module algorithm is specially designed according to the image generation theory of the optical fingerprint collection device. It has excellent correction & tolerance to deformed and poor-quality fingerprint. It has a high-powered DSP chip that does the image rendering, calculation, feature-finding, and searching. It is connected to the microcontroller with a TTL serial, it then sends packets of data to take photos, detect prints, hash and search.

It can enroll new fingers directly-up to 162 fingerprints can be stored in the on board FLASH memory. Its operating current is a less than 80mA (120mA max) which is good for the occasion in which the security system is powered by a battery.



Fig.2: SM630 Fingerprint module.

B. Arduino Uno microcontroller board.

The Arduino Uno based on the AT mega 328 microcontroller is chosen among other kinds of microcontroller as the control unit of the system because of its unique features such as 14 digital IO pins, 6 analog input pins, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains an embedded programmer that supports the microcontroller; it is simply connected to a computer with a USB cable when the written program code is ready to be burnt. The USB

cable will supply the Arduino with a regulated 5v DC input voltage while the Arduino is being programmed. This saves the stress and cost of getting a separate external programmer for the AT mega 328 microcontroller the Arduino uses.

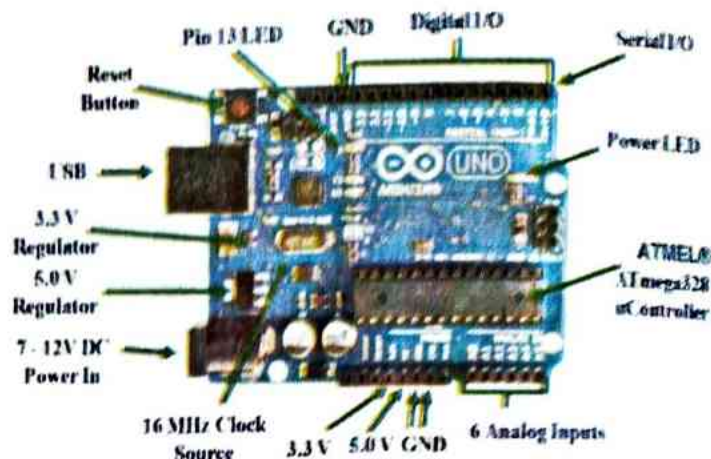


Fig.3: Arduino Uno, R3 board.

C. Liquid crystal Display (LCD) unit.

This shows the output message to the user during fingerprint verification, it is used in a 4 bit data mode. The LCDs have a parallel interface, meaning that the microcontroller has to manipulate several interface pins at once to control the display. The interface consists of the following pins;

A register select (RS) pin that controls where in the LCD's memory you're writing data to. You can select either the data register, which holds what goes on the screen, or an instruction register, which is where the LCD's controller looks for instructions on what to do next.

A Read Write (R/W) pin that selects reading mode or writing mode

An Enable pin that enables writing to the registers 8 data pins (D0 -D7). The states of these pins (high or low) are the bits that you're writing to a register when you write, or the values you're reading when you read.

The process of controlling the display involves putting the data that form the image of what you want to display into the data registers, then putting instructions in the instruction register. The Liquid Crystal Library simplifies this for you so you don't need to know the low-level instructions.

The Hitachi-compatible LCDs can be controlled in two modes: 4-bit or 8-bit. The

4-bit mode requires seven I/O pins from the Arduino, while the 8-bit mode requires 11 pins. For displaying text on the screen, we do everything in 4-bit mode, so the circuit in Figure 18.2 shows how to control a 2x16 LCD in 4-bit mode. Additionally, we wire a 10K pot to +5V and GND, with its wiper (output) to LCD screens V0 pin (pin3), and the backlight pins: A to +5v, and K to ground.

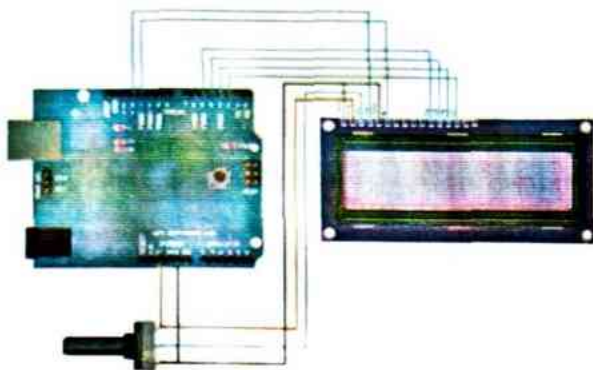


Fig.4: Connection for the LCD display to the Arduino microcontroller.

D. Electromechanical solenoid lock.

The Electromechanical lock used in this work uses D.C voltage operated solenoids to actuate the lock. Solenoid locks were chosen for this work because all it needs to be activated is a 12v DC.

Initially, on default, the solenoid bolt provides locking of the cabinet by driving its bolt into the strike preventing the cabinet door from opening. Whenever a right fingerprint is matched, the solenoid becomes activated by current from the pin of the microcontroller interfaced with a power transistor to the lock itself; therefore it becomes magnetized and attracts the bolt out from the lock hole, so that the cabinet opens.

POSITIVE & NEGATIVE TERMINAL CABLES



Fig 5 Solenoid electromechanical lock.

E. Keypad buttons

For selection of the various fingerprint functions such as searching fingerprint, adding fingerprint and deleting fingerprint, keypads made of button switches would be used because of its simplicity and ease with which it can be interfaced with hardware components such as resistors.

When each button switch is pressed, it allows a specific analog voltage value to be seen at the analog input pin A0 of the Arduino microcontroller, the microcontroller then makes its decision of searching, adding, or deleting a fingerprint based on the analog value of the voltage received.

The value of the analog voltage by each button pressed is determined by chosen different values for the pull up resistors.

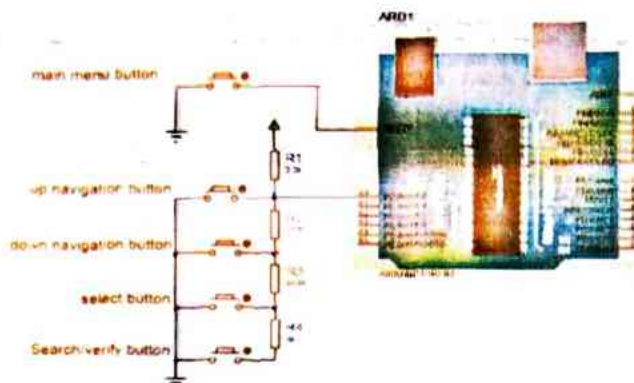


Fig.6: Circuit connection of keypad button switches to Arduino board.

F. Buzzer

The buzzer used is an active buzzer, this is chosen because an active buzzer only requires an external DC voltage to make it sound which is what we need for our project since the whole system is driven by a 12v power supply. The buzzer sounds an alarm for a short duration when the fingerprint entered does not match any fingerprint stored in the fingerprint database. It is activated when it receives a digital high from the output pin of the microcontroller.

G. Power supply unit

This project requires a 12v power supply to power the microcontroller board, the electromechanical lock, buzzer, the 12v needed is supplied from A.C to D.C power converter, while a 12 battery is kept as backup and is charged up whenever through a charging circuit.

4.0 System Implementation and Result

4.1 Hardware design

The method of implementing the project involves developing each unit separately from other units at the end of which the whole unit is integrated together to form a whole system. Each unit added to the system must be tested before advancing to the next stage. This method is especially important in cases where system may develop a faults since it would be much easier to trouble shoot each individual unit than the whole system at once. The units to be implemented separately are:

A. The input units (fingerprint module)

- The four output wires of the sensor were first soldered to the vero board.
- The positive and negative terminals of the fingerprint module are soldered to the power and ground lines respectively with the aid of a jumper wire.
- The RX and Tx wire then soldered to the digit pins 1 and 0 of the Arduino board.

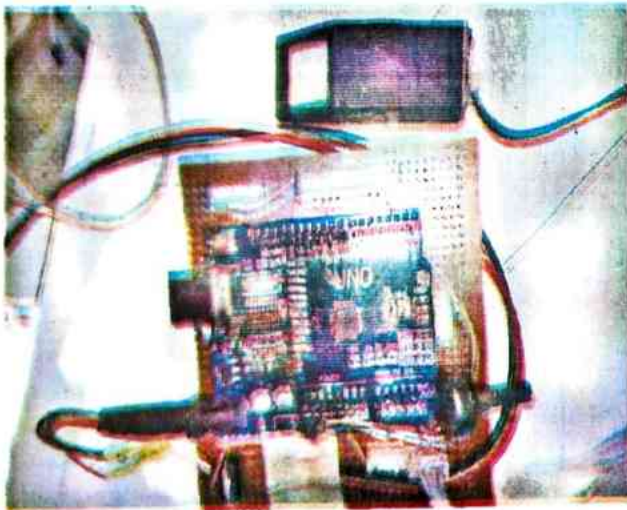


Figure 7: Arduino Uno, T3 board.

B. The LCD Units

- The register selects and Enable pins of the LCD are soldered to pins 12 and 11. The read write is soldered straight to ground, using jumper wires.
- Pins D4-D7 of the LCD is soldered to the Arduino pins 5,4,3 and 2 respectively. we use only 4 data pins since we operate the LCD on a 4 bit mode of save I/O pins.

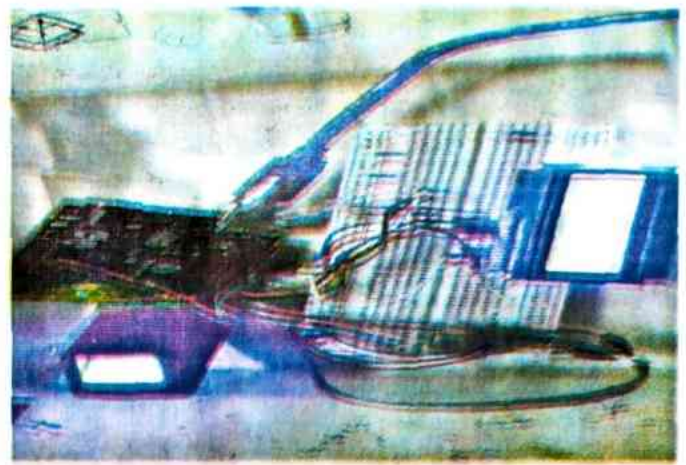


Figure 8: Arduino Uno, R3 board

C. The output Unit (electromechanical lock and buzzer)

- The two terminals of the electromagnetic lock is soldered to the collector of a bc337 transistor whose base is soldered to pin 10 of the Anduino with a base resistor of 10k in between.
- A flywheel diode is soldered in parallel to the lock that protect the lock against back e.m.f from the solenoid lock.
- The buzzer is driven by another BC337 transistor driven by pin 10 of the Arduino through a 10k resistor.

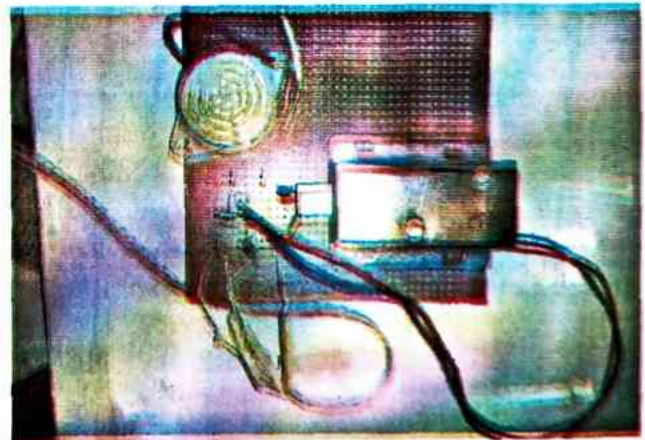


Figure 9: Output Unit: Solenoid lock with buzzer

A. Hardware units

- Input unit (SM630 fingerprint module, Keypad input).
- Control unit (Arduino Uno microcontroller).
- Output unit (LCD, buzzer, electromechanical lock).

4.2 Software Design

- Fingerprint enrollment software code.

- Fingerprint verification software code.
- LCD display software code.

The software was developed using C-language. It was developed in an Arduino IDE

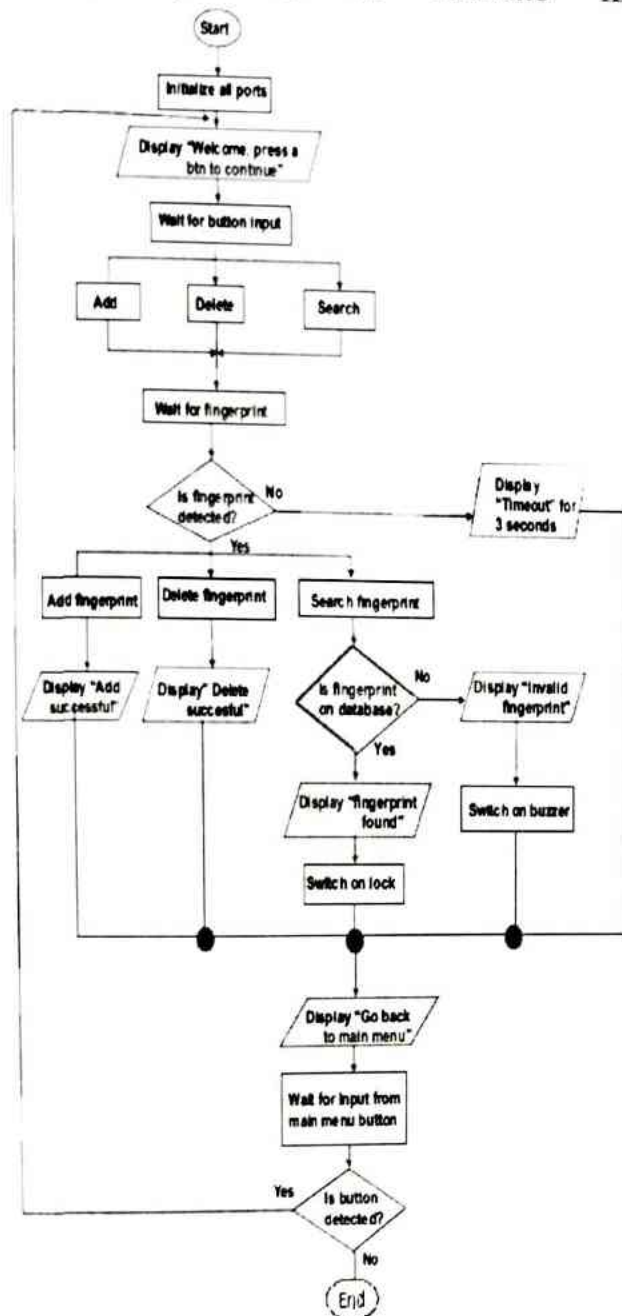


Figure.10: Flow chart design for fingerprint verification and cabinet lock.

4.3 System Testing

In this stage the individual units has been integrated to form the complete system. The program is burnt into the microcontroller and plugged into the socket already soldered on the Vero board. The system was connected to AC and monitored to ensure the required performance. Searching for fingerprint (see fig.11)

This is the one function of the control device that lets the lock open in order to gain access into the cabinet.

1. Place your finger on the fingerprint sensor
2. Press the **search button** while your finger is still on the fingerprint sensor and wait for a few seconds while it searches for your fingerprint.
3. If your fingerprint was previously registered, the cabinet unlocks, but if your fingerprint is not registered a buzzer sounds to indicate an unauthorized fingerprint and the cabinet remains locked.
4. Once access is gained into the cabinet as it unlocks, a new fingerprint can be registered or an old fingerprint deleted using the buttons at the back of the packaging.

Adding fingerprint

1. Once access has been gained into the cabinet, the user can then use the buttons at the back of the control box to add a new fingerprint.
2. To add a new fingerprint use the **UP/DOWN navigation buttons** to navigate to the "add fingerprint option".
3. Once you are in the "add fingerprint option", select it using the **select button** and with your finger still on the fingerprint sensor, wait for a few seconds while its adds your fingerprint.
4. After your fingerprint has been successfully added, press the Fig.5: Solenoid electromechanical lock **main menu button** to go back to the main menu.

Deleting Fingerprint

1. Once access has been gained into the cabinet, the user can then use the buttons at
2. The back of the control box to delete an old fingerprint.
3. To delete a registered fingerprint, use the **UP/DOWN navigation buttons** to navigate to the "delete fingerprint option".
4. Once you are in the "delete fingerprint option". Select it using the **select button** and with your finger still on the fingerprint sensor, wait for few seconds while its deletes your fingerprint.
5. After your fingerprint has been successfully deleted, press the **main menu button** to go back to the main menu.

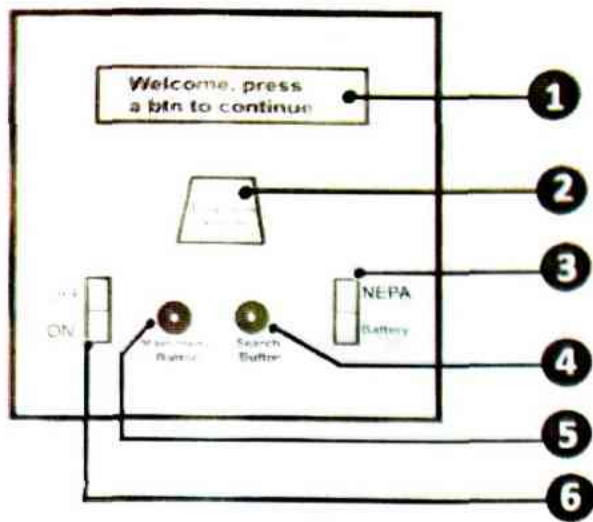


Fig.11: Front view of control panel.

General Description (Fig.11)

- 1 – LCD display
- 2 – Fingerprint Sensor
- 3 – Change Over switch
- 4 – Search button
- 5 – Main menu button
- 6 – on/off Up/Down switch

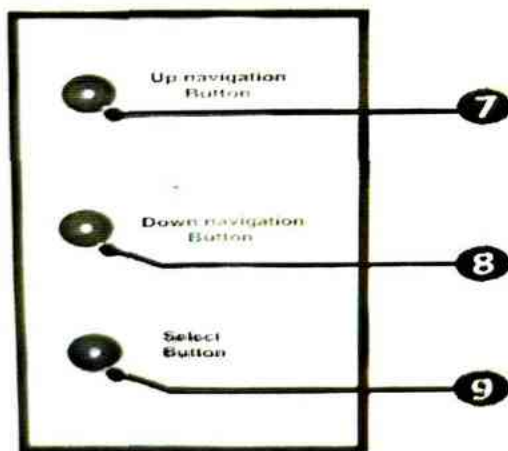


Figure 12: Back view of control panel.

General Description (Fig. 12)

- 7 – Up Navigation buttons
- 8 – Down Navigation button
- 9- Select button



Figure 13 : Finished work.

4.4 System Evaluation

The system is programmed in such a way that when the right fingerprint is entered, the cabinet lock opens and, but if the wrong fingerprint is entered, an alarm sounds for a short time while the red LED comes on. In both cases, the user is prompted accordingly through the LCD display.

Table.1: Evaluation of the system

Test cases	Observation	Result
When the system is powered ON.	LCD displays "waiting for fingerprint", and green LED comes on.	The cabinet Remains locked.
When a registered fingerprint is entered.	LCD displays "Access granted",	The cabinet Lock opens.
When an unregistered fingerprint is entered.	LCD displays "Access denied",	The cabinet Remains locked.

5.0 Conclusion

The fingerprint based biometric cabinet lock is very efficient, less complex and meets the security needs of the modern time. It provides more security for an office cabinet than a traditional deadbolt lock. It also provides keyless entry and is nearly impossible to pick thereby providing users with a stronger sense of security and as the most commonly known and widely used biometric security system, the growing use of fingerprint reading will inevitably revolutionize the security aspects of our daily life in the nearest future.

References

- [1] Wildes, R.P., "An Emerging Biometric Technology", IEEE Computer Magazine, Volume 85, Issue 9, (2004), pp. 1348-1363.
- [2] Jain A.K., Prabhakar s., Hong l., Pankanti s., "filter bank-based fingerprint matching", IEEE Trans. Image Process. 9(5), (2000), pp. 846-859.
- [3] Saleh A.A., Adhami R.R., "curvature-based matching approach for automatic finger print identification", 2001, pp.171-175.
- [4] A. Aditya Shankar, K. sastry, A.L. vishuram, A. vamsidhar. "Fingerprint Based Door Locking System", International Journal of Engineering and Computer Science (IJECS) ISSN: 2319-7242, volume 4, issue3, march 2015.
- [5] Tomas Bulka and Chaitanya Agarwal, "Secure Mobile Identification System", (2005), pp.3-19.
- [6] Voice Recognition Security System by Xiaowen lu and shihjia lee, Department of electrical and Computer Engineering, Cornell University, New York, USA, 2006.

Authors Profile

➤ Ufoarah Stephen U. is a lecturer at the department of Electronic and Computer Engineering. His research interest is on Communication and Control Engineering. He is a registered Engineer with Council for regulation of Engineering in Nigeria (COREN) and a professional member of the institute of Electrical and Electronics Engineers (IEEE). He can be contacted via e-mail sufufoarah@yahoo.com or call +2348035018583.

➤ Okonkwo Obikwelu R. is an Ass. Professor of Computer Sc with background in Computer Engineering. He has interest in Information Technology and Data Security. He has published in so many journals on Computer forensic, data management and security, IT application and virtual system.

➤ Christopher Ogwugwuam Ezeagwu is a lecturer in the department of Electronic and Computer engineering Nnamdi Azikiwe University Awka. He holds a master degree in engineering (communications). Currently a research student in optic fibre at Enugu State University of science and Technology. A registered member of Council for Regulation in Engineering (COREM). Nigeria Society of engineers

(NSE). Member Institute of Electrical Electronic Engineers(IEEE). A fellow institute of chartered Administrator of Nigeria

➤ Erike Uzoma C. is a B.Eng holder in the Electronic and Computer Engineering from Nnamdi Azikiwe University, Awka, Anambra State, Nigeria. His areas of interest include software design and implementation, Modeling and simulation of Automatic Control systems, Instrumentation and measurements, Artificial Neural Networks, Design and construction of mechatronic system and many other areas. He is a student member of the Nigerian Society of Engineers (NSE).