Implementation of Fingerprint Based Biometric Security System Using Arduino-Uno

Ibrahim M. Harram[1], Hamza Abba[2], Victor Daniel[3] and Patrick ThankGod[4]

[1] Department of Computer Engineering Technology
[2, 3, 4] Department of Electrical and Electronics Engineering Technology
School of Engineering Technology
The Federal Polytechnic, Damaturu, Yobe State

Correspondence e-mail: imharram@yahoo.com

Abstract
The concept of Fingerprint based Biometric Security is related to the security issues in the day to day life. The physical key can be made as duplicate in very cheap cost and the key can be lost somewhere or it can be stolen. To overcome these issues we can use biometric security gadgets and try improvise the security much more because it can never be stolen it cannot be lost and the stealing chance of duplication are very low to break the security. Components such as Arduino-Uno, finger module were used for the implementation of this project. A keypad is also used to add or delete the valid user in the module. FIM3030 fingerprint module. Arduino is used for controlling the whole driving unit. LCD is used as a displaying unit for showing the information about the authorized and unauthorized user. It can be concluded that fingerprint security system is a better alternative to use than the paper card to efficiently reduce the chance of entry by unauthorized people. Hence the aims and objectives of the project were achieved.

Keywords: **Fingerprint, Biometric, Security, Arduino-Uno, Authentication, Recognition**

I. Introduction

Biometrics refers to the automatic identification of a living person based on physiological or behavioural characteristics for authentication purpose. Among the existing biometric technologies are the face recognition, fingerprint recognition, finger-geometry, hand geometry, iris recognition, vein recognition, voice recognition and signature recognition, Biometric method requires the physical presence of the person to be identified. This emphasizes its preference over the traditional method of identifying what you have such as, the use of password, a smartcard etc. Also, it potentially prevents unauthorized admittance to access control systems or fraudulent use of ATMs, Time Attendance Systems, cellular phones, smart cards, desktop PCs, Workstations, vehicles and computer networks.

The ancient Egyptians and the Chinese played a large role in bio-metrics history. Today, the focus is on using biometric face recognition, iris recognition, retina recognition and identifying characteristics to stop terrorism and improve security measures. This section provides a brief history on biometric security and fingerprint recognition. During 1870, Alphonse Bertillon developed a method of identifying individuals based on detailed records of their body measurements, physical descriptions and photographs. This method was termed as “Bertillon-age” or anthropometrics and the usage was aborted in 1903 when it was discovered that some people share same measurements and physical characteristics. Sir Francis Galton, in 1892, developed a classification system for fingerprints using minutiae characteristics that is being used by researchers and educationalists even today. Sir Edward Henry, during 1896, paved way to the success of fingerprint recognition by using Galton's theory to identify prisoners by their fingerprint impressions.

Biometric recognition systems offer greater security and convenience than traditional methods of personal recognition. Fingerprint recognition represents the oldest method of biometric identification which is dated back to 2200 BC. The use of fingerprints as a personal code has a long tradition and was already used. This system focuses on the use of fingerprints for door opening and closing. The fingerprint recognition software enables fingerprints of valid users of the vehicle to be enrolled in a database. Before any user can use the vehicle, his/her fingerprint image is matched against the fingerprints in the database while users with no match in the database are with regard to automated fingerprint recognition technology, there exist well-known limits related to processing performance (i.e. how fast it can be done), to accuracy (i.e. how reliable the result of a comparison is) and to handling (i.e. the level of expertise necessary for its use).

However, there is also a limit with respect to aging. Bio-metric identifiers (including fingerprints) have in common that they are based on physiological properties which may change over time. For the particular case of fingerprints, it is assumed that the characteristic pattern obtained from each finger is absolutely unique and unchanged for lifetime but at least the size of the pattern grows from childhood to adulthood.

This security system is one of the most rising technologies that have largely drawn the attentions of the people due to its effectiveness in reducing impersonation and some other forms of crime. For instance, in the universities, polytechnics, colleges of education and other tertiary institutions where exam malpractices are rampant through impersonation, fingerprint based security system can be employed to address this issue effectively. Apart from academic application of this system, it can also be employed in accessing a computer, a network, an ATM machine, a car and a home.

Finger print based security system is most secured as compared to other systems. Reason is that RFID card or keys on lock can be stolen, password may be leaked. However, thumb print of every human being is unique, so lock will not open unless the same person is present to give the impression of finger print.

Biometric security.

The term “Bio-metrics” is derived from the Greek words “bio” (life) and “metrics” (to measure) (Kumar & Ryu, 2009). Automated biometric systems have only become available over the last few decades, due to the significant advances in the field of computer and image processing. Although biometric technology seems to belong in the twenty first century, the history of bio-metrics goes back thousands of years.

Fingerprint Recognition System.

Fingerprint imaging technology has been in existence for centuries. Archaeologists have uncovered evidence suggesting that interest in fingerprints dates to prehistory. In Nova Scotia petroglyphs (from the time of pre-historic Native Americans) showing a hand with exaggerated ridge patterns has been discovered. In ancient Babylon and China, fingerprints were impressed on clay tablets and seals. The use of fingerprints as a unique human identifier dates back to second century B.C. China, where the identity of the sender of an important document could be verified by his fingerprint impression in the wax seal (Kumar & Ryu, 2009). In fourteenth-century Persia fingerprints were impressed on various official papers. At that time, a governmental official observed that no two fingerprints were exactly alike. Using the newly invented microscope, Professor Marcello Malpighi at the University of Bologna noted ridges on the surface of fingers in 1686. He described them as loops and spirals but did not note their value as a means of personal identification.

II. Review of Related Literature

In developed countries, the system finds application while conducting examination as a process of verifying students’ fingerprints for their eligibility to writing examinations. This work highlights the development of fingerprint verification. Verification is completed by comparing the data of authorized fingerprint image with incoming fingerprint image. Then the information of incoming fingerprint image will undergo the comparison process to compare with authorized fingerprint image. In this project, digital image processing algorithms is employed to identify whether the incoming fingerprint image is genuine or forgery (Saxena, Bisen & Bhoyerker, 2012). Furthermore, this system incorporates finger print module, together with liquid crystal display (LCD) in order to ensure effectiveness of its performance.

In the research paper “Fingerprint based locking system”, (Mishra et al., 2015) says that fingerprints are patterns of ridges and valleys on the surface of the finger. Like everything in the human body, these ridges form through a combination of genetic and environmental factors. The genetic code in DNA gives general orders on the way skin should form in a developing fetus, but the specific way it forms is a result of random events. With the help of interfacing, fingerprints can be used to create secure and impenetrable door locks and several lock systems. Interfacing is a method of establishing communication between Microcontroller and the Interface. Fingerprint interfaces are generic and can communicate with any microcontroller. It is a combination of hardware (i.e. the Interface) and Software (i.e. the source code to communicate, also called as the Driver). In simple words, to use LED as output device, it should be connected to a port pin of the microcontroller with a program running inside the microcontroller to make it ON/OFF or blink or dim. This program can be developed using any programming language like Assembly, C, Basic etc.

Security doors have been implemented using different methods such as Radio frequency identification (RFID) and Biometric lock to unlock and lock door. Both the RFID and biometric lock are real ideal and smart ways to make a door smart, due to necessity and limitations such as cloning of biometric prints or card. The use of Bluetooth and smartphone is much simpler and easier to adapt and use. It gives more access to communicate with the door and it also give access to physically challenged persons that might not have a finger to use for biometric lock or is crippled to use RFID. With this project, physically challenged can simply open their door by single click in device.

(Zhang, Liu & Chen, 2011) did a similar project Android based smart door locking system which also employed the use of android phone which is also a smartphone and also a GSM module to access the door. (Sankaranayan, Wan & Pusa, 2014) did android based automation and security system for smart homes. There are many others done on smart door in different countries. They are all different from each other in terms of designs, features, devices, and algorithm. They are mostly designed according to specific needs and availability of components in the respective areas. Some of them are cheap; some of them are very expensive. Availability of both hardware and software is necessary to work. After a long searching, I have found a lot of articles. Searching for security purpose articles, also found some projects done for door security. These are mainly done in western countries. Many projects are done only for security purpose With Arduino or Raspberry Pi. Again, the projects are done only for controlling home Appliances using Arduino or Raspberry Pi. Most of the previous researches encountered problems in their design especially in terms of cloning by other third party and availability of components ed Intelligent relay coupled door control system using technology.

Kumar & Ryu (2009) talks about the classification of a security system interface. According to him, the security system using fingerprint interface can be divided into the following Modules:

1) Fingerprint analysis software module that accepts fingerprints images;
2) Hardware interface module and the locking system module.

He (author) further added, stepwise break-up of execution plan looks like the following,

1) Study of biometrics literature - especially with reference to fingerprint analysis.
2) Study of basics of image processing algorithms so as to compare images with the point of view of unique-ness of fingerprints.
3) Cogitation of MATLAB as a programming tool for image processing and comparing.

Mishra et al., (2015) opined that, “fingerprints are one of many forms of biometrics, used to identify individuals and verify their identity”.” The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern”. “These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns.” According to him, it is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical. He added that the three basic patterns of fingerprint ridges are the arch, loop, and whorl. In his description- Arcs are the ridges that enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger. Loops are the ridges that enter from one side of a finger, form a curve, and then exit on that same side. Last but not the least, he says that whorl are ridges that are formed circularly around a central point on the finger. In the whorl pattern, ridges form circularly around a finger.

Kumar S. (2014) in his paper ‘A smart door access system using finger print biometric system’, quotes that previously, for high security areas or in locker rooms for banks, traditional lock systems, passwords, etc., were employed. However, these systems were found to be not perfectly secure. After advancements in technology RFID cards were used. These cards however were not much useful for the user due to chances of getting lost, stolen and forgotten. The purpose of this study is to provide high security for such high end security applications. The aim of this study is to design a smart door access system using finger print module. The use of this device is to provide access to only authorized persons. Both hardware and software technology are used to design it. An emergency beep sound is provided to protect the system by giving alarm if any unauthorized person intrudes into the system. An indicator indicates for any emergency condition. Motors are used for locking and unlocking the door.

III. Drawback in Review

A smart door access system using finger print biometric system was used for high security areas or in locker rooms for banks, traditional lock systems, passwords, etc., were employed. However, these systems were found to be not perfectly secure. After advancements in technology RFID cards were used. These cards however were not much useful for the user due to chances of getting lost, stolen and forgotten. The purpose of this study is to provide high security for such high end security applications.

This project implement the Construction of a fingerprint based biometric security system with door locking with the used of microcontroller will be aimed at eliminating the above limitations i.e the use of RFID cards which has the disadvantage such as getting lost, stolen and forgotten. This project has high level of security which recognizes the uniqueness of fingerprint which is not limited to ageing.

IV. Implementation and Construction Method

This chapter illustrates the implementation of a fingerprint based biometric security system with door locking. It explain the methodology and procedures of design with microcontroller, materials and it principles of operation.

Based on the design principle, a change in the direction of current flow reverses the direction of rotation. Thus, the motor was connected in the switching unit to lock and unlock the safe when its supply current is switched in different directions. During the construction 5v servo was implemented and the following values were obtained from data sheet.

$$I_T = I_c + I_a + I_f$$

Where I_a is the armature current = 10mA

I_f Is the field current = 0.4mA

I_c Is the collector current = 100mA

$$I_T = I_c + I_a + I_f = 10\text{mA} + 0.4\text{mA} + 100\text{mA} = 110.4\text{mA}$$

Power of Motor

$$P_M = V_{dc} \times I_T$$

$$= 4.9 \times 110.4\text{m}$$

$$= 540.96\text{mW}$$

Speed of motor

$$\text{N} = \frac{9.55 \times E \times I}{T}$$

Rated max %torque, T = 50% = 0.5

$$\text{N} = \frac{9.55 \times 4.9 \times 110.4 \times 10^{-3}}{0.5}$$

$$= 618\text{rpm}$$

V. Choice of Components

Fingerprint

Research on biometric methods has gained renowned attention in recent years brought on by an increase in security concerns. The recent world attitude towards terrorism has influenced people and their governments to take action and be more proactive in security issues. This need for security also extends to the need for individuals to protect, among other things, their working environments, schools, homes, personal possessions and assets. Many techniques have been developed and are being improved with the most successful being applied in everyday law enforcement and security applications.

Finger Print Sensor (R305)

This is a finger print sensor module with TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter. The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person. The FP module can directly interface with 3v3 or 5v Microcontroller. A level converter (like MAX232) is required for interfacing with PC serial port.

Optical biometric fingerprint reader with great features and can be embedded into a variety of end products, such as: access control, attendance, safety deposit box, car door locks (Sharaf, Bashir, 2016).

Features

i. Integrated image collecting and algorithm chip together, All-in-One

ii. Fingerprint reader can conduct secondary development, can be embedded into a variety of end products

iii. Low power consumption, low cost, small size, excellent performance

iv. Professional optical technology, precise module manufacturing techniques

v. Good image processing capabilities, can successfully capture image up to resolution 500dpi

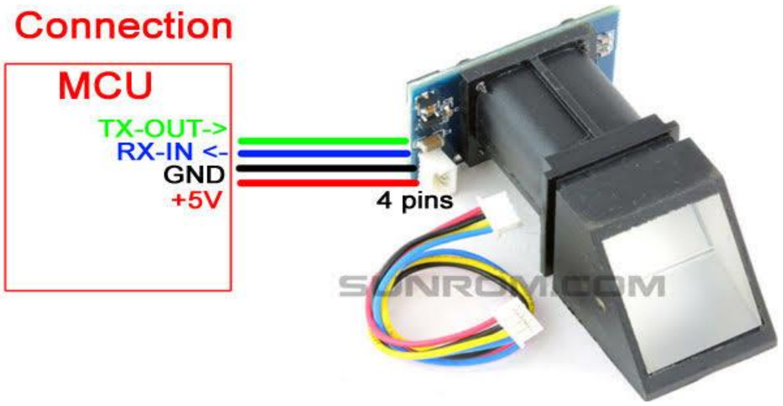

Figure 1: Finger print Sensor

Arduino UNO

The Arduino Uno is a microcontroller board based on the ATmega328 (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started. "Uno" means one in Italian and is named to mark the upcoming release of Arduino 1.0. The Uno and version 1.0 will be the reference versions of Arduino, moving forward. The Uno is the latest in a series of USB Arduino boards, and the reference model for the Arduino platform.

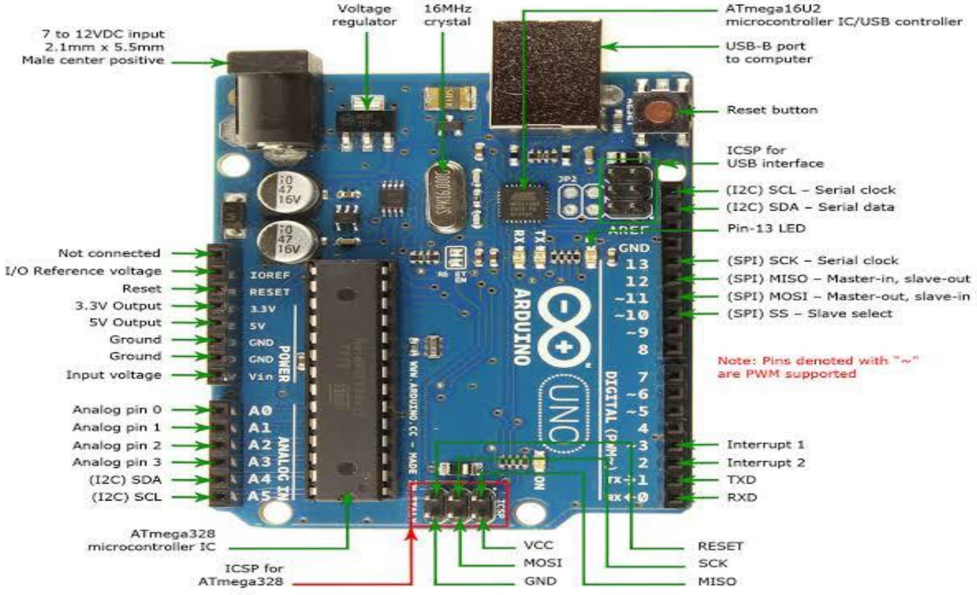

Figure 2: Arduino Board

The Liquid Crystal Display (LCD)

Liquid crystal display is an electronic display module that finds a wide range of application in circuits. It is preferred over seven segment and other multi LED because it is more programmable and economical. A 16*2 LCD means it can display 16 character per line and there are 2 such lines.

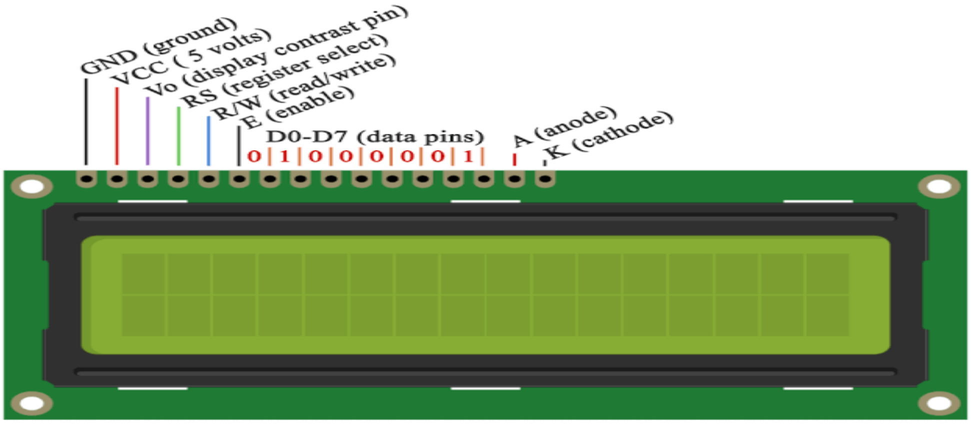

Figure 3: Liquid crystal display (LCD)

List of all Components/materials required

i. Arduino
ii. Switch
iii. Finger print module
iv. LCD

Breadboard Layout

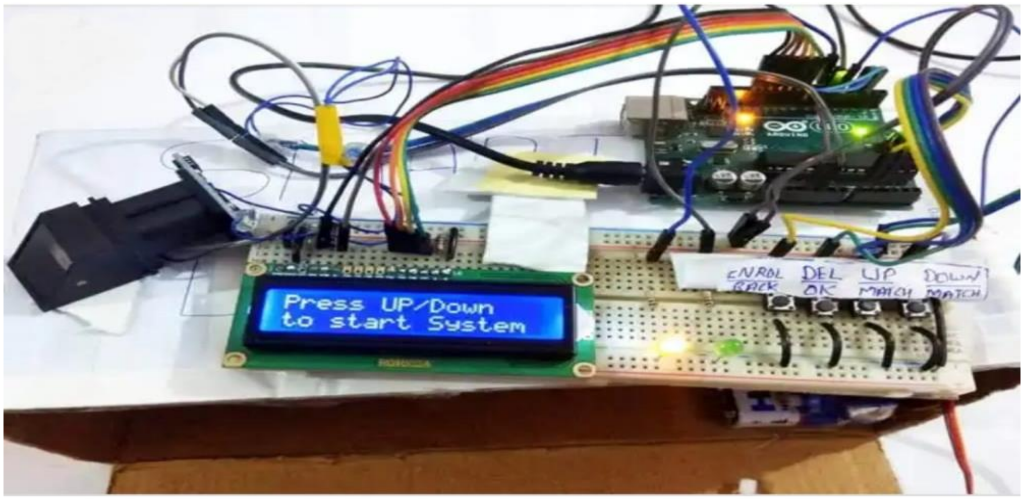

Figure 4: Breadboard Layout

PCB/Vero Board Layout and Soldering

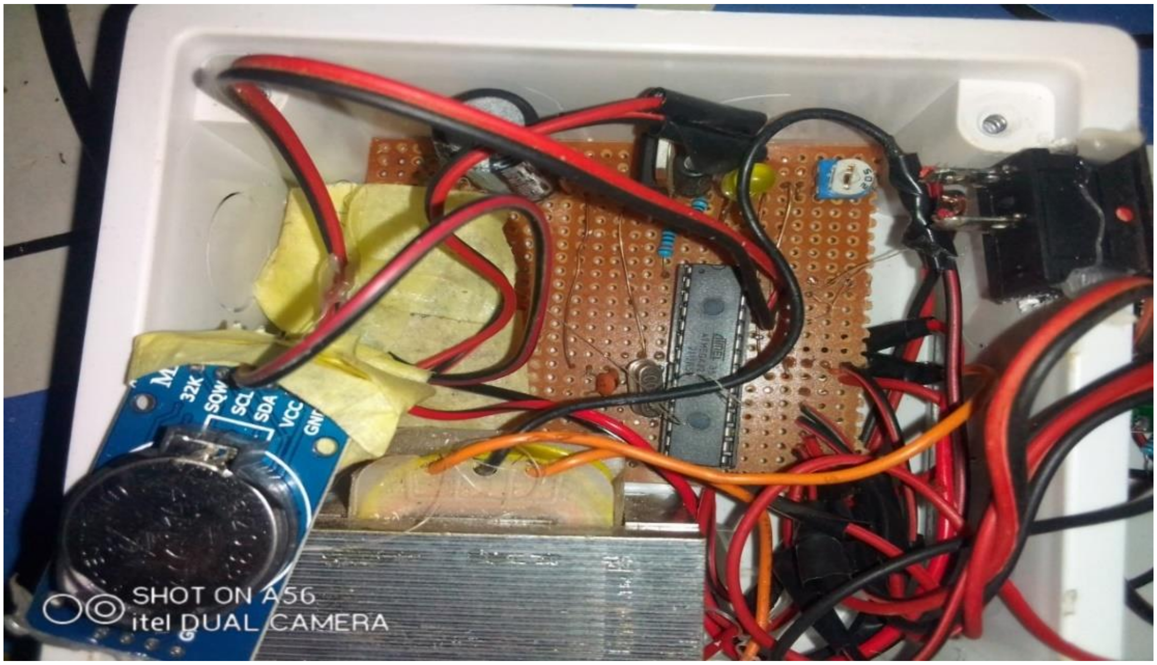

Figure 5: Veroboard and Soldering Layout

System Assembly and Casing

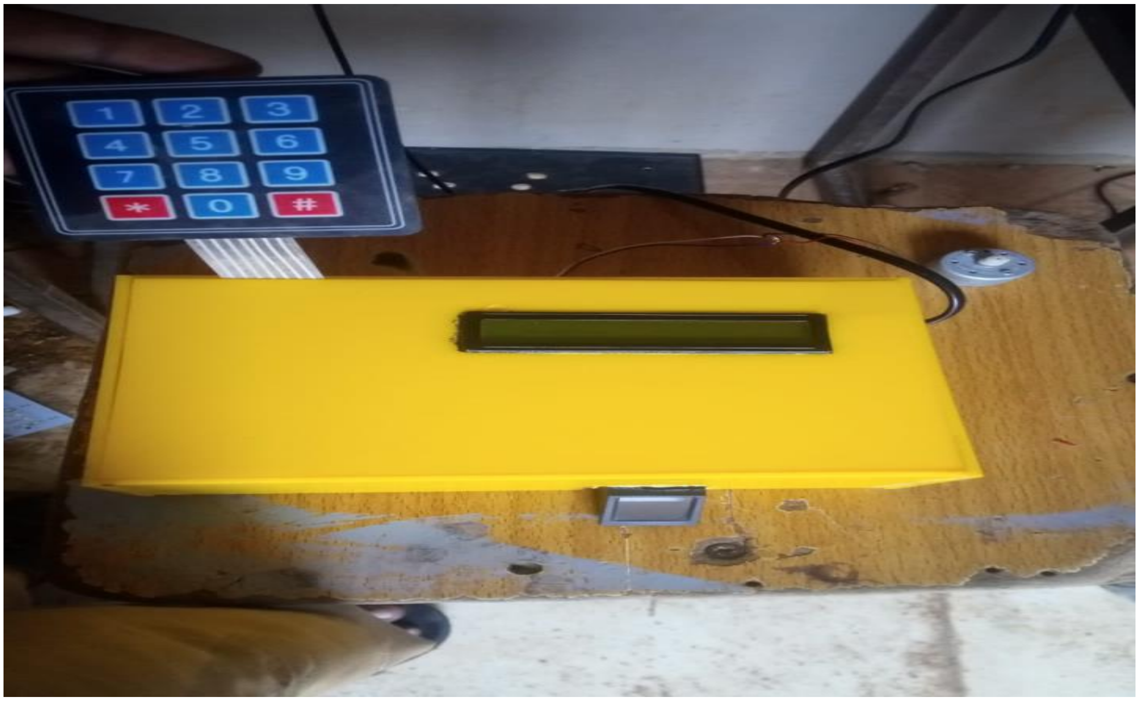

Figure 6: Complete System Casing

VI. System operational principle

The operation starts as soon as the system is powered. The LCD displays ‘Design and Construct of a fingerprint based biometric security system with door locking’ as this is displayed, the microcontroller will search for the available module and Network. After which the microcontroller will send signal to the LCD to display ‘place your finger’. The user will then place his registered finger on the fingerprint sensors, the sensor will then capture the image of some crucial features of his fingerprint, process them and send them to the microcontroller. Microcontroller will then compare the user’s fingerprints with the one stored in it. If the two fingerprints correspond, electrical signal (current) will be sent to the transistor through the base, the signal will then drive the transistor to saturation. After the transistor has been driven to saturation current flows through the collector to the relays. At this stage one of the two relay will be ON which will allow the door to open for authentic user. The process will repeat itself and the second relay becomes ON while the first becomes OFF this will make the door to close after some delay. A flywheel diode is placed across the collector to prevent the backflow of the current when the relay is OFF to prevent the backflow current from damages the transistors.

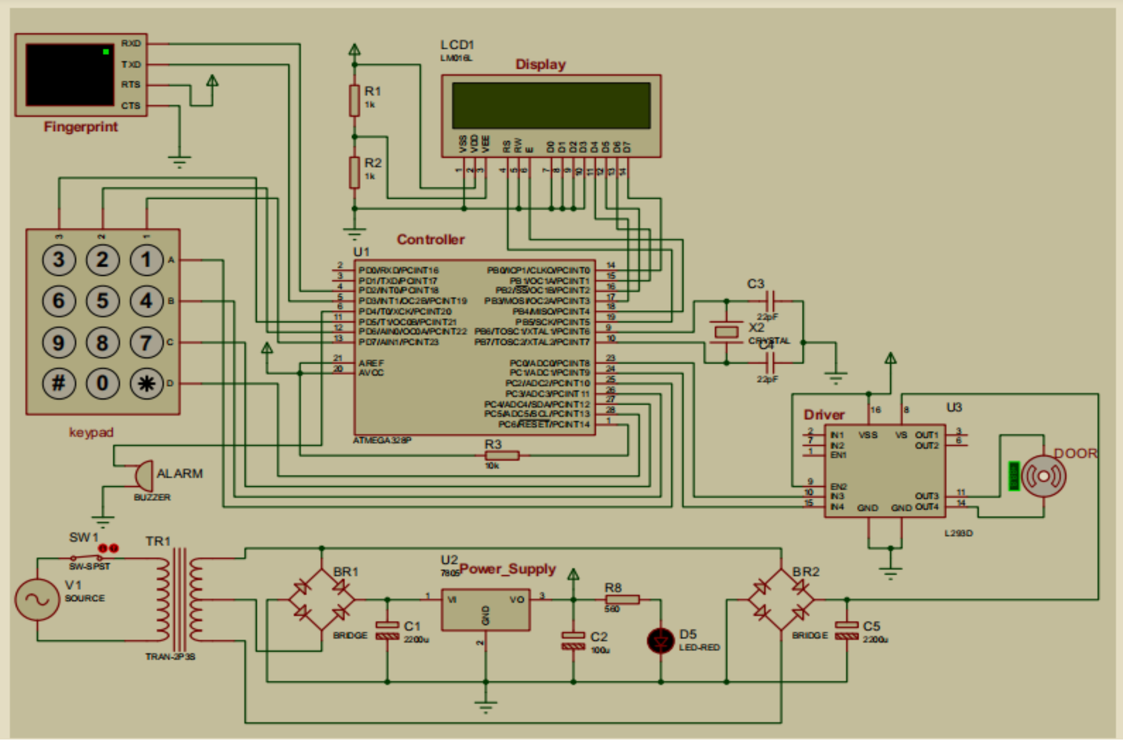

Figure7: Projects Circuit Diagram

When the user places his registered finger on the fingerprint sensor, the microcontroller triggers the sensor to capture the images of some crucial features of the fingerprints and then process them. The sensor then sends back the images to the microcontroller the microcontroller compare the incoming fingerprints with the one in the program whether they match or not. If they do (YES), the door opens then the program comes to an end. Otherwise (NO). Hence the program goes back to the initial stage.

VII. Test, Results and Discussion

This discusses the design implementation of the system which is the hardware structure which comprises of microcontroller and finger print module.

Test schedule

The components used for the implementation of this project were tested on breadboard for better performance, and were later transferred to the Vero board and soldered. The heat applied during soldering was just moderate to avoid damage of the Vero and the components since most of the components have low heat resistance. The test equipment includes;

i. Breadboard-To assemble and test individual components
ii. Digital multi meter to measure voltage, current, resistance and check for continuity
iii. Arduino sketch

Results

Result obtained for the power supply unit

Table 1 Power Supply Unit Result

Transformer	Theoretical Voltage(V)	Measured Voltage(V)
Output voltage	12	11.4
Rectifier LM317	4.2	4.02
Rectifier LM7805	5	5.01

VIII. Discussion of result

The table shown above presents the results obtained from the tests carried out on power supply unit circuit. The test results are of two categories; theoretical voltage value test results and measured voltage value test results. It was found that the theoretical input voltage value of the transformer varies from its measured voltage value by 5V. It was also observed at the output that the theoretical output voltage value of the transformer varies from the measured output voltage by 0.6V.

Also for the regulator, it was observed that the theoretical input voltage value of the regulator varies from the measured voltage value and the same thing applies to the output values of the regulator. The reason for these variations might be do loss of electrical energy. The power supply unit of +5V and +12V were tested for the output voltage under no-load and full-load conditions.

Under no-load, the voltage of +5V supply section was measured to be 5.0V while that of the +12V supply was measured to be 12.00V. At full-load, the respective voltages were measured as 4.8V and 11.7V.

Voltage Regulation (V.R) is given as

$$V.R = \frac{V_{NL} - V_{FL}}{V_{NL}} \times 100\,\%$$

Where;$V_{NL} = No - load\ voltage$

$V_{FL} = Full - load\ voltage$

For the units operating on +5V,

$$V.R = \frac{5.0 - 5.05}{5.0} \times 100\% = 1.00\%$$

For the units operating on +12V

$$V.R = \frac{12.0 - 11.4}{12.0} \times 100\% = 5.00\%$$

$V.R = 5.00\%$ Reason for the variation;

For the units operating on +4.2V

$$V.R = \frac{4.2 - 4.02}{4.2} \times 100\% = 4.28\%$$

$$V.R = 4.28\%$$

IX. Conclusion and Recommendation

Fingerprint based door locking system has been successfully designed and working. This system consists of an Arduino Uno board, finger print module. The system, also used for security of the entry into a particular structure. In this paper focuses on the fingerprint security as every person has unique fingerprint.

Conclusion

After the design and implementation of the project, it is found that only the authorized people whose fingerprints are enrolled and registered in the fingerprint module are recognized by the system. Therefore, it can be concluded that fingerprint security system will be a better alternative to use than the paper card to efficiently reduce the chance of entry by unauthorized people. Hence the aims and objectives of the project were achieved.

Recommendation

For further work on this topic, the following measures can be carried out to improve its functionality.

1. The use of face recognition systems should be employed in place of fingerprint for efficient control of unauthorized entry.
2. A camera should be incorporated for visual monitoring of entry into the building.

References

Kumar Dileep, Ryu Yeonseung, (2009), A brief introduction of Biometric and Fingerprint Technology, International Journal of Advanced Science and Technology, Vol4, pp. (30-32).

Mishra Pragyang, Prof. Pujari Sashank, Singh Sumit, Yadav Kumar Devendra, 2015, Finger prints based attendance system using microcontroller and Labview, International Journal of Advanced Research, Vol 4, Number 6, pp. (512- 515).

Zhang Jinhai, Liu Xinjian, Chen Bo, "The design and implementation of ID Authentication System Based on Fingerprint Identification", 2011 Fourth International Conference on Intelligent Computation Technology and Automation

D. Saxena, P. Bisen and S. Bhoyerkar. 2012. Development of Intelligent Security and Automation System, International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE). 1: 139- 143.

S. Kumar, 2014. Ubiquitous Smart Home System Using Android Application. International Journal of Computer Networks and Communications (IJCNC). 6: 33-43.

S. Sankaranarayanan, A.T. Wan and A. H. Pusa, "Smart Home Monitoring using Android and Wireless Sensors", I.J. Engineering and Manufacturing, vol. 2, pp 12-30, Aug 2014. URL:http://.android.com/about/versions/index.html.

V. Madan and S.R.N. Reddy, "GSM-Bluetooth based Remote Monitoring and Control System with Automatic Light Controller", International Journal of Computer Applications, Vol. 46, No 1, pp 20-28, May 2012

http://circuitdigest.com http://electronics.howstuffworks.com

http://www.creativeworld9.com/2011/04/abstract-andfullpaper-on-bluetooth.html