Engineering and Technology Journal e-ISSN: 2456-3358

Volume 07 Issue 07 July-2022, Page No.-1376-1382

DOI: 10.47191/etj/v7i7.08, I.F. – 6.484

© 2022, ETJ

Biometric Access Control Using Voice and Fingerprint

Boluwatife Christianah Abe[1], Haonat Olajumoke Araromi[2], Emmanuel Segun Shokenu[3], Peter Olalekan Idowu[4], Joshua Dada Babatunde[5], Monsuru Abolade Adeagbo[6], Itanrin Hope Oluwole[7]

[1,2,3,5,6] Department of Computer Engineering, Ladoke Akintola University of Technology (LAUTECH), Ogbomoso, Nigeria

[4] Department of Electronic and Electrical Engineering (EEE), Ladoke Akintola University of Technology (LAUTECH) Ogbomoso

[7] Adekunle Ajasin University Akungba Akoko, Ondo, Nigeria

Orcid Id: [2]0000-0002-7546-8762, [3]0000-0002-2780-1268, [4]0000-0002-1099-1691, [5]0000-0002-7546-8762.

ABSTRACT: In security-related systems, such as access control systems, authentication is extremely important. There are several ways to carry out this crucial activity, but biometrics is currently attracting more attention. After realizing the usefulness of biometrics, security systems use them for one of two fundamental functions: user identification or user verification. Multiple biometrics exist, and various access control systems require various biometrics. As a result of their impossibility to be lost, stolen, or forgotten, biometrics have been deemed the most secure and practical authentication method. Therefore, the design and development of the voice and fingerprint-based magic access control system. This research explores the idea of increasing access control door security by replacing a door key with a trustworthy electromagnetic door lock system that allows only authorized people to access a location using voice recognition or a fingerprint device. The voice sensor and fingerprint sensor were able to scan the user's voice or fingerprint to open a prototype door when a valid user try to access the door. The motor closes the door after a preset 5 seconds delay.

KEYWORDS: Fingerprint, a voice sensor, Electromagnetic lock, ATMEGA328 microcontroller, Power Supply, Relay.

I. INTRODUCTION

Security has become increasingly crucial over time as concerned people, businesses, and organizations work to increase the safety of people and their possessions [1]. A security system is defined as detecting intrusion, or unauthorized entry into a building or a protected area and denying such unauthorized access to protect personnel and property from damage or harm. Security systems are mainly used in residential, commercial, industrial, and military properties for protection against burglary (theft) or property damage, as well as personal protection against intruders [9].

The words "Bio" and "Metric" are Greek words that imply life and "measure," respectively. The term "biometric" can be described as the measurement (research) of life, which includes people, animals, and plants, by combining these two words. The term "automatic ways of validating or recognizing the identity of a live individual based on a physiological or behavioral feature" refers to biometric technology as a whole [1]. They have been exposed to contemporary technology for Access control and identification. The distinguishing and quantifiable traits that are used to label (distinguish between Individuals) and describe individuals are known as biometric identifiers. Physiological and behavioral traits are common categories for biometrics. The shape of the body is related to physiological traits. Examples include fingerprints, palm veins, facial recognition, deoxyribonucleic acid (DNA), palm prints, hand geometry, iris/retina patterns, and body odor. Behavioral features, on the other hand, are acquired traits that an individual possesses and are connected to their pattern of behavior. They consist of typing rhythm, walking gait, disposition, and voice [5].

In automatic security systems generally, passwords, identification cards, and PIN verification techniques are being used, however, these methods have the drawbacks of being vulnerable to hacking 2 and having cards stolen or lost. Studies on biometrics frequently involve the recognition and validation of hand geometry, iris, voice, face, fingerprint, and other biometrics. The development and evaluation of numerous other modalities are still ongoing. An excellent mismatch ratio, high-security accuracy, and dependability are some of the best qualities that the fingerprint demonstrates [14]. In China, fingerprinting was first used in the fourteenth century. Although the use was most probably as a signature, the fingerprint's potential to be uniquely identified was not fully understood. Dr. Henry Fauld originally considered fingerprints as a method of criminal identification after he discovered them on antique pottery while working in Tokyo [13]. When an impression is left on a touched surface, the friction ridge arrangement found on the tips of the fingers is reproduced, and this is what is referred to as a fingerprint. The fingerprint meets the requirements for optimal biometrics (i.e., It must be universal, unique, permanent, and collectible). There is a very high mathematical possibility that no two fingers will ever match because no two fingerprints may have the same print [5].

Voice recognition, commonly referred to as automatic speech recognition (ASR) or Speech to Text (STT), is a branch of computational linguistics that focuses on recognizing the speaker and decoding the human voice. Voice recognition has recently found use in telephone, automobile systems, education, access control systems, and other areas. Virtual assistant software is being employed in smartphones and many forms of devices to carry out various tasks or commands. One of the many biometrics applications with many applications in access control systems is voice recognition. According to [2], voice recognition (32 %), fingerprints (27 %), facial scans (20 %), hand geometry (12 %), and iris scans (10 %) were discovered to be the top five biometric measurements for consumer preference According to this report, consumers strongly favor voice recognition biometric systems [2].

II. REVIEW OF RELATED WORKS

Security systems have been developed in several locations over the years. In daily life, security measures are essential. Some of the researchers have successfully done the study and created numerous security systems kinds employing diverse technologies. Some authors were emphasized in this area, along with the concepts and theories behind their works. The benefits, drawbacks, and areas for development (the research gap) were also enumerated. [9] Uses RFID technology to create a digital door lock security system. The reader transfers the data it receives from the tag to the database for verification. If it does, the data is saved for use at a later time. After receiving the reader's question, the central server makes a query to the database and retrieves the pertinent data. After receiving the server's reply, the reader calculates the timestamp (date, time), then produces a log. After the tag information is confirmed, the system generates a control signal over a parallel connection that instructs a stepper motor to open and close the door. Another crucial security element of the system is the creation of a log that includes user information, however, it lacks alerting and alarming features. The system can be improved by adding security features such as a GSM module and buzzer.

A storage locker system was implemented by [10]. The system activates the opening and closing of the lock using the fingerprint recognition approach. Although biometric security is dependable, it does not provide protection for physically disabled persons (such as amputees) or a way to alert the authorities in the event of an intrusion. By incorporating additional security measures, such as an RFID system, the system's security can be improved.

[7] Designed an autonomous access control system based on RFID. The host computer, which is connected to the PIC 16f877A, was communicated using USB serial connection. Therefore, the graphic user interface application, which was created using visual basic 2010, offers the functionality of the total system, including showing live ID tag transactions, registering, removing, and recording attendance. The system is more adaptable because it has the ability to register and delete IDs, but it lacks features for actual user authentication, such as a fingerprint scanner or camera. RFID fingerprint scanners can be used in place of Tags in this system as an enhancement to eliminate the potential of unwanted entry. [12] Designed a security door that could be unlocked by either entering the corresponding code on a computer set that was interfaced with the system or by hitting the keys of the supplied codes on a mobile phone. When the correct code is entered, the door automatically opens and stays open for ten seconds before shutting again. The security system is reasonably priced but does not have an automatic code generating or registration mode mechanism. The addition of biometric, auto-generation and registration mode mechanisms can be improved.

A system that imitates an electronic key was designed by [11] and was operated using a Bluetooth-enabled smartphone. The Arduino circuit, which serves as a conduit between the Android smartphone and solenoid, is controlled by sending a command over Bluetooth to it. There is no alerting system, despite the security system's simplicity and low failure rate. To improve the security system's dependability, modification can be done by including an additional security feature.

[3] Developed a GSM-based approved access system with a separate user password control system for doors. Data is sent using a GSM modem by an SMS application. Another GSM phone with a receiving end connection feeds data to the microcontroller. If the supplied data (the user's password) matches the password that is stored in the microcontroller, the microcontroller starts a mechanism to unlock the door through a motor driver interface. The program in the microcontroller lacks an auto-generated code procedure, despite the fact that it is straightforward and will provide a decent return on investment. The microcontroller's ability to create codes can be improved.

A biometric locker system with a short messaging service was created by [4] using a microcontroller (SMS). The locker is unlocked once the fingerprint scanning mechanism compares it to the previously saved pattern. When an unfamiliar fingerprint was found, the worldwide system for mobile (GSM) module was able to send a text message giving the locker's automatically generated passcode. The system has no registration mode mechanism to register the finger pattern of a new user, but it is still an easy and dependable technique to secure a lock system. To enhance security reliability, registration mode can be added, along with other security measures.

III. MATERIAL AND METHODS

The designing and construction of biometric access control using voice recognition and fingerprint is centered on two biometric traits authorized to improve security and reduce the possibility of compromising safety. The system design consists of hardware design and software design, implemented together to actualize well-secure access control. Figure 3.1 depicts the block diagram of the system in figure 3.2. The system has several hardware components such as the ATMEGA328Microcontroller, Fp10A fingerprint sensor, ISD1700 voice sensor, Bluetooth receiver, relay, Power Supply Unit, Vault mechanism, and some other electronic or electrical components. The software consists of code that would be compiled on the Arduino IDE and embedded into the microcontroller; it would be a part of the hardware design.

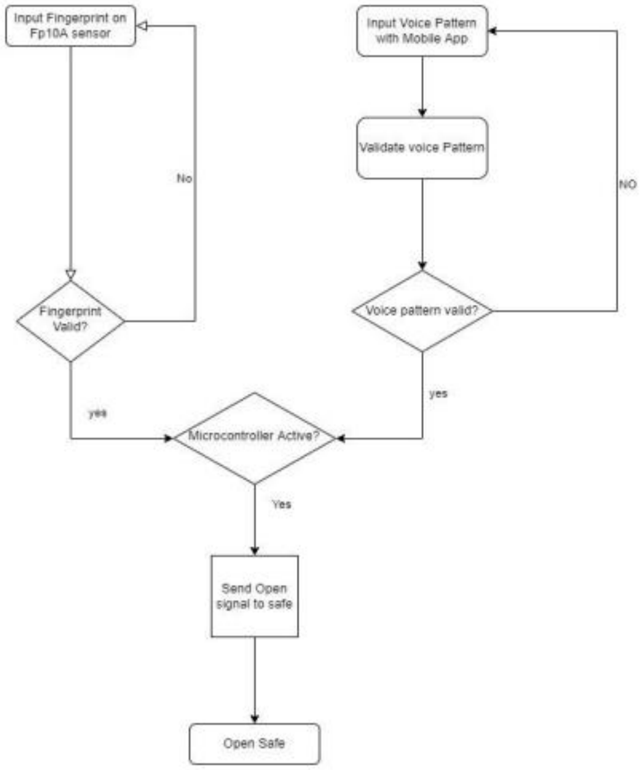


Fig. 3.1 System Flowchart

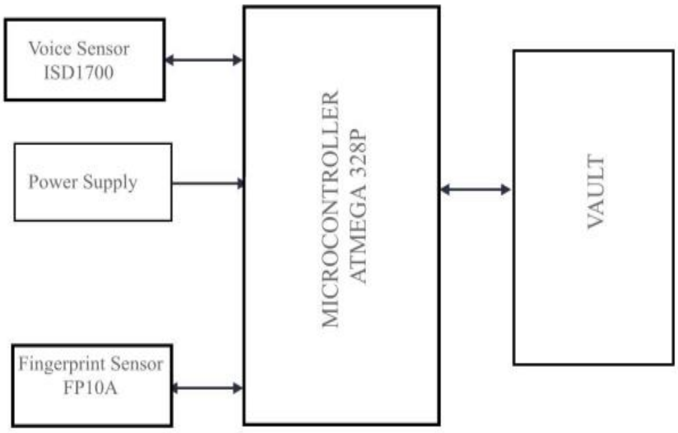


Fig. 3.2 Block Diagram biometric access control using voice recognition and fingerprint.

3.2 Hardware Requirements

3.2.1 Power Supply Unit

This unit was designed to supply DC voltage and current to the whole constructed circuit. In the construction of this power supply, a step-down transformer was used to step down the input voltage of 220Volt to 12Volt, a full-wave bridge rectifier was used for rectification of the voltage, which convert the 12VAC to 12 VDC, then a capacitor is used to filters out the pulsating AC voltage that is not fully converted. The power supply is connected to the outlet socket on the wall supplying unregulated AC voltage, and the output pin is connected to the input pin (Vin) of the voltage regulator. The regulator modulates and regulates the 12VDC to give a constantly regulated 5Volt needed by the microcontroller and provide the other electronic component used in the circuit designed their exact standard operating voltage, however, this is done to prevent damages to the microcontroller ICs and other component used from excess supplied voltage.

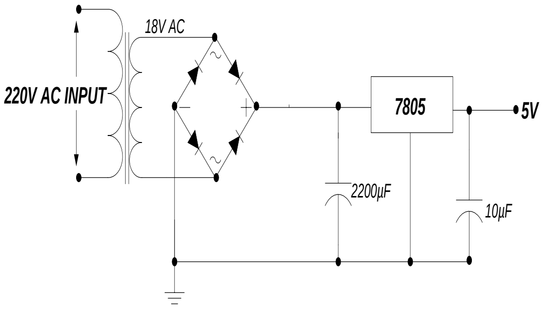


Fig. 3.3. Circuit diagram of the Power Supply Unit

3.2.2 Regulating Unit (LM7805)

A circuit's voltage sources could change, causing variable voltage outputs. The output voltage is kept constant using a voltage regulator integrated circuit (IC). A well-known integrated circuit is the 7805 Voltage Regulator, which is one of the 78xx series of fixed linear voltage regulators designed to maintain such variations (IC).

The power supply's output voltage is changed by the LM7805 IC to the 5V needed by the ATMega328p microprocessor. The output of the voltage regulator is connected to the 5V pin of the ATMega328p microcontroller, while the input of the voltage regulator is connected to the output of the power supply, the ground of the voltage regulator is connected to the ground of the microcontroller, and the negative voltage of the power supply.

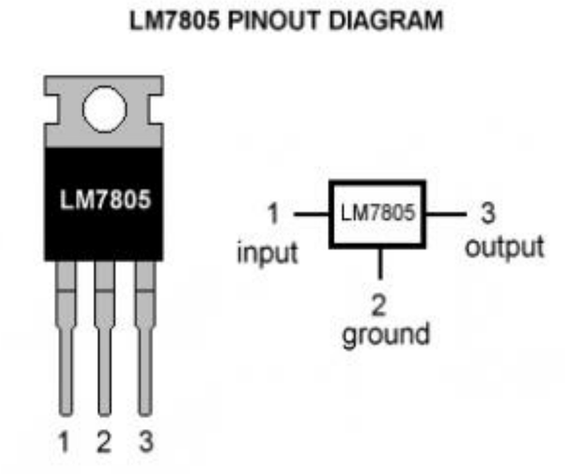


Fig. 3.4. Diagram of the Voltage Regulator (LM7805)

3.2.3Microcontroller Unit (ATMega328p)

This unit control and oversee the operations of the embedded system, this component, which functions like a compressed microcomputer, is programmed in C. The high-performance, low-power Microchip 8-bit AVR® RISC-based microcontroller combines 32 KB of ISP flash memory with read-while-write capabilities, 1 KB of EEPROM, 2 KB of SRAM, 54/69 general-purpose I/O lines, 32 general-purpose working registers, a JTAG interface for boundary-scan and on-chip debugging/programming, three flexible timer/counters with compare modes, internal and external From 1.8 to 5.5 volts are needed to run the device. The ATmega-328 is the most well-liked device on the market right now thanks to its many features. These characteristics include a sophisticated RISC architecture, good performance, low power consumption, a real-time counter with a separate oscillator, six PWM pins, a programmable Serial USART, a programming lock for software security, throughput of up to 20 MIPS, etc.

Fig. 3.5 Diagram of the ATMega328p Microcontroller

3.2.4 Transistor Switching Stage

The output of the ATMega328P microcontroller controls the relay's switching via a transistor switching stage, which then switches power to the door latch. The power of the load that needs to be triggered depends on the relay contact rating; as a result, the relay you choose is very important. In class-A mode, the transistor functions as a switch. When the microcontroller emits a HIGH output, the relay is turned on. To guarantee flawless transistor switching in saturation, a base resistor is necessary. The diode shields the transistor from any reverse emf that may be produced by the inductive load that the relay coil represents. The resistance of the relay coil in this instance is R, which is the collector resistance, and it is 400 for the relay type used in this project.

3.2.5 Fingerprint Sensor (Fp10A)

The Fp10A fingerprint sensor is utilized to both confirm the authenticity of the individual's claimed identity as well as to acquire an individual fingerprint image for use at the enrollment stage. One benefit of this fingerprint sensor is its low cost and simplicity of use. It also has a self-adaptive adjustment mechanism that enhances the quality of both dry and wet fingers. The biometric enrolment stage, where the fingerprint is taken to be stored in a database, and the identification or authentication stage, where the already registered fingerprint is checked for a match in the database with the new input to grant access to the vault, will be the two stages involved in the operation of this system. The system was designed to go in a systematic way through a predetermined order of stages. The fingerprint sensor module that was utilized in this project has six incredibly thin wires, but only four of them were useful for connecting to the microcontroller; two of these lines will be used for power and two for data. The VCC and GND were linked to the 31 microcontrollers' respective VCC and GND pins, and TX and RX were connected to the Atmega328 microcontroller's RX (digital pin 2) and TX (digital pin 3) pins. White wires for DNC Red wire: VCC Blue wire TX Green wire for RX The black wire is GND.

Fig 3.6. Fingerprint module (FPM10A)

3.2.5.1 Fingerprint Registration Stage

Every individual that wants to get authenticated to access the vault system must first of all enroll. The process involves the use of the FP10 fingerprint scanner to acquire the fingerprint of the user, creating templates of the images after segmenting, extracting the unique features, and normalizing the images.

When enrolling, the individual entered the fingerprint on the scanner, the system processed the fingerprint image, generated a template of the finger based on processing results, and stored the template. The flowchart for the enrolment stage is shown in Figure 3.7.

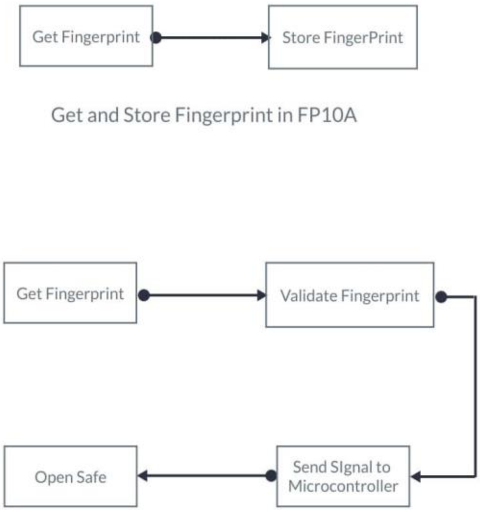


Fig. 3.7 Fingerprint Process

3.2.5.1 Fingerprint Identification and Authentication Stage

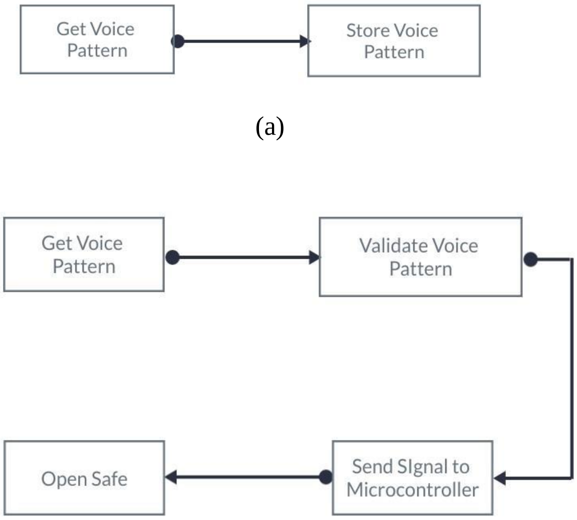
Once the individual has been enrolled into the system the individual is then given access to the vault. Identification simply means a one-to-many match requiring the user to provide the fingerprint as a means of identification. The user enters the registered fingerprint on the fingerprint scanner, the just acquired biometric sample presented for identification is compared to the previously stored sample in the database and a signal is sent to the microcontroller to see if there is a match. If there is a match with the fingerprint enrolled, access is provided to the vault, access is confirmed by the flashing of the green LED light, and otherwise, it is declined 32 which is alerted by a flashing red LED light. The flowchart for the Identification stage is shown in Figure 3.7.

3.2.6 The Voice Recognition

The voice recognition method to open the vault was achieved in two ways through the ISD1700 Voice Sensor that was used to store and retrieve user voice data/pattern, validate the pattern and send appropriate signals to the microcontroller to open the vault as shown in figure 3.9. The user registers their voice pattern on the first use by speaking their preferred voice pattern into the microphone, which is connected to the ISD1700 voice sensor as shown in figure 3.9(a). The user registers 2 recordings of the same voice pattern, this is done to improve the matching accuracy. The registered voice pattern is then saved for future reference. After registration. The user activates the microphone on the sensor and speaks to it. The sensor then validates the pattern with the stored voice pattern and provides access accordingly.

Photo by ElectroPeak

Fig. 3.8 ISD1700 Voice module



(a)

(b)

Fig. 3.9. Voice Process using ISD1700 voice sensor

4.0 RESULT AND DISCUSSION

In this designed project, the microcontroller was programmed in C language to control the opening of the vault system using a fingerprint module by placing a finger on the sensor to validate fingerprint whether to open the safe or to keep it locked. At initial use, the individual will register their fingerprint and save it in the memory of the device, so that when it is time to open the vault, all they have to do is to place their fingerprint on the sensor, and it will automatically run a validation check with the fingerprint pattern stored in the memory. After this validation, the sensor will send a signal to the microcontroller to signify that a match has been found, this signal will then be transmitted to the magnetic relay to reduce the voltage from 12 v, which is the high voltage that powers the magnet, to 5 volts, the low voltage that allows the vault to open. If the vault is not open within 5 seconds, the microcontroller sends a signal to the relay to arm itself, thereby locking the vault. It is also programmed to control the opening of the vault system using voice recognition by voice sensor ISD1700 by speaking to the microphone to validate the voice pattern to signal the microcontroller to open the safe, and the cycle can be repeated over and over.

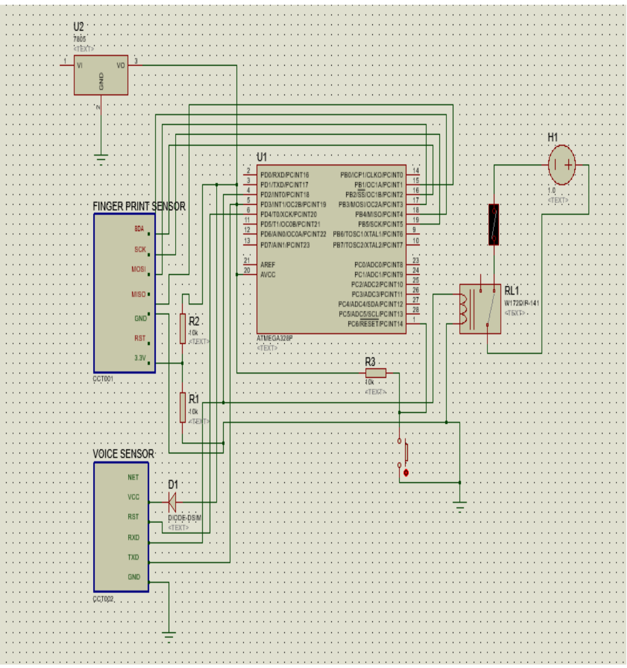


Fig. 4.1. Circuit Diagram of biometric access control using voice recognition and fingerprint.

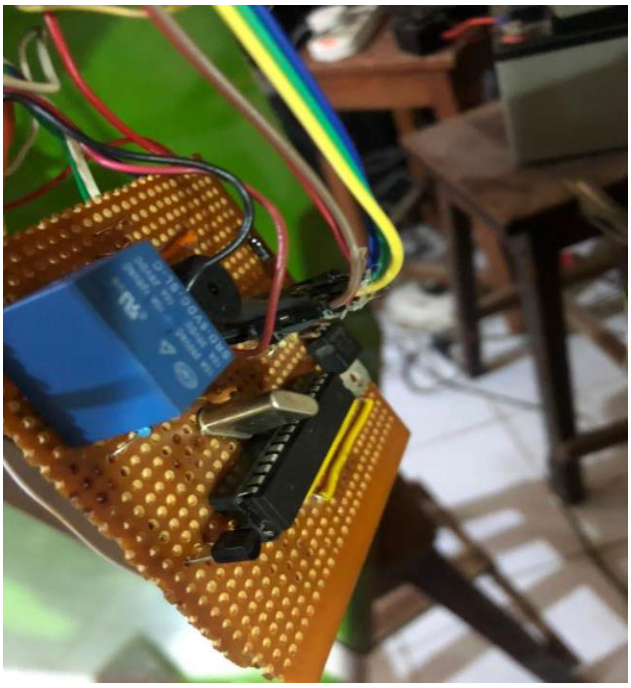


Fig 4.2 Microcontroller Circuit.

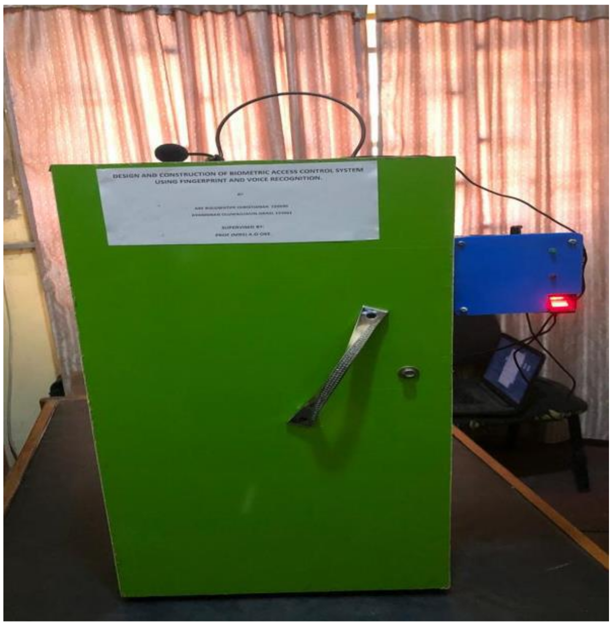

DESIGN AND CONSTRUCTION OF BIOMETRIC ACCESS CONTROL SYSTEM USING FINGERPRINT AND VOICE RECOGNITION

Fig.4.3. Idle state of the device

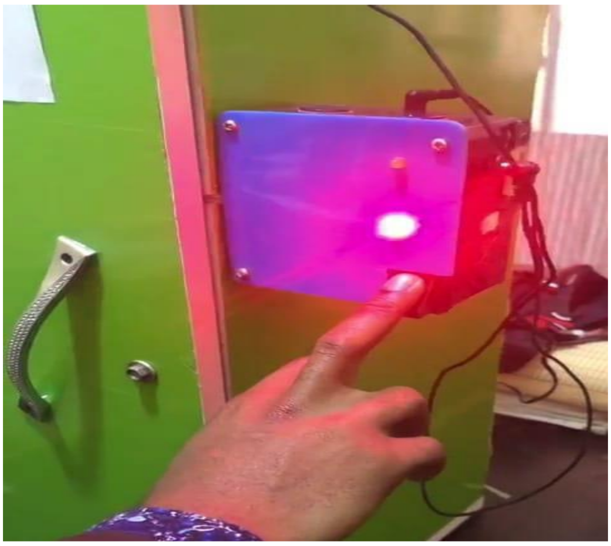


Fig.4.4 Unauthorized access prompt

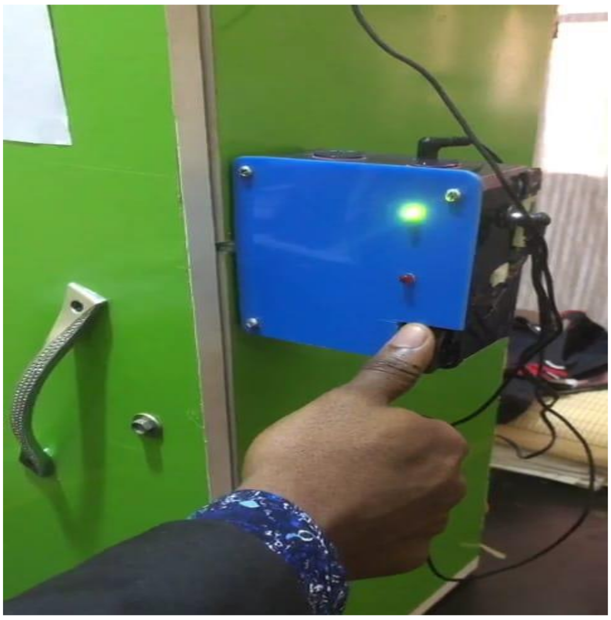


Fig.4.5 Image of Successful Verification

CONCLUSIONS

This project, which entails the design and construction of biometric access controlled safe with voice and fingerprint access, was planned with consideration for a number of variables, including cost-effectiveness, economy of design, accessibility to parts and research materials, effectiveness, and compatibility, portability, and longevity. Project execution after testing met design requirements. However, the whole performance and functionality of the project rest on the user's willingness to accept human error, such as providing an incorrect voice or fingerprint, and there is flexibility for updates whenever voice models can be reliably validated, and the construction was done in a way that makes maintenance and repairs a straightforward task and economical for the user should there be any system breakdown.

REFERENCES

1. A Rashid, Rozeha & Mahalin, Nur & Sarijari, mohd adib & Aziz, Ahmad. (2008). Security system using biometric technology: Design and implementation of Voice Recognition System (VRS). 898 - 902. 10.1109/ICCCE.2008.4580735.
2. Adekola,Olubukola, D., and Somefunolawale, M. (2019). Voice Recognition Door Access Control System. October. https://doi.org/10.9790/0661-2105010112 .
3. Algae L. R., Algae, A. and Sivakumar, P. (2015). GSM-based authorized access with separate user password door lock and unlock control system, International Journal of Electrical and Electronics Engineers (IJEEE). 07(01), 388-391.
4. Crystalline, D. C., Jaswinder, S. B., Jocelyn, R. H., Ditched, J. C. A., Melvin, S. D. C. and Jairam, C. I. (2016). Development of Microcontroller-Based Biometric Locker System with Short Message Service” Lecture Notes on Software Engineering. 04(02), 103-106.
5. Ezeoba E.O, Ogherohwo E.P(2016).Design and Construction of a Biometric Examination Authentication Device.
6. Etinosa Noma-Osaghae, Kennedy Okokpujie, Olatunji Okesola, Osemwegie Omoruyi Chi-nonso Okereke, Samuel John and Imhade P. Okokpujie.(2018).Fingerprint Bio metric Authentication Based Point of Sale Terminal.
7. Geoffrey, C. T. S. (2012): Automatic Access Control System using Student Identification Card Based on RFID Technology, Unpublished Undergraduate Project of Faculty of Electrical Engineering University Technology Malaysia, 1-4.
8. Gyanendra, K. V. and Pawan, T. (2010). A Digital Security System with Door Lock System Using RFID Technology, International Journal of Computer Applications. 05(11),6-8.
9. Karimi, K., Kabrane, M., Zohr, I., Hassan, O., Badouch, A., Zohr, I., and Krit, S. (2020). Secure Smart Door Lock System based on Arduino and Smartphone App. 12, 407–414. https://doi.org/10.5373/JARDCS/V12SP1/20201088.
10. Lay, Y. L., Yang, H. J. and Tsai, C. H. (2011): Biometric Locker System, Proceedings of the World Congress on Engineering and Computer Science (WCECS) 2011, San Francisco, USA.01, 1-4.
11. Lia, K, Alfin, N. S. R, Made S. W. S. and Edi, M. (2014): Door-Automation System Using Bluetooth-Based Android for Mobile Phone, Asian Research Publishing Network (ARPN) Journal of Engineering and Applied Sciences.09(10), 1759-1762.
12. Nwankwo, P. N., Sion, I. I. and Ezeli, C. J. (2013). Design and Implementation of Microcontroller Based Security Door System (Using Mobile Phone and Computer Set), Journal of Automation and Control Engineering, 01 (01), 65-69.
13. Patricia Melin, Janusz Kacprzyk, Witold Pedrycz.(2010).
14. Soft Computing for Recognition Based on Biometrics. Studies in Computational Intelligence, Volume 312, DOI 10.1007/978-3-642-15111-8.
15. Rahman, A., Chowdhury, M. E. H., Khandakar, A., Tahir, A. M., Ibtehaz, N., Hossain, M. S., Kiranyaz, S., Malik, J., Monawwar, H., & Kadir, M. A. (2022). A robust biometric system using session invariant multimodal EEG and keystroke dynamics by the ensemble of self-ONNs. Computers in Biology and Medicine, 142, [105238]. https://doi.org/10.1016/j.compbiomed.2022.105238