

Journal of Civil and Environmental Systems Engineering

Department of Civil Engineering, University of Benin, Nigeria

*Journal homepage: <https://j-cese.com/>***DESIGN AND CONSTRUCTION OF A FINGERPRINT SECURITY DOOR WITH INFRA-RED REMOTE CONTROL AND GSM ALERT SYSTEMS.***Okoye, J.U. and Osemekhian, O.**Department of Computer Engineering, Faculty of Engineering, University of Benin, Nigeria**Corresponding authors: jokoye360@gmail.com and Osemekhian.omoifo@uniben.edu***Abstract**

This study presents the design and construction of a fingerprint security door with infra- red remote control and GSM alert systems. This was done to modernize the previous normal system, making it more efficient, user- friendly, and feature-rich thus enhancing its usefulness. One of the basic challenges of the fingerprint security system is that the fingerprint of an individual can change, making identification and verification difficulty. When the fingerprint of an individual is damaged, the fingerprint patterns will be altered; thus, making authentication impossible. The fingerprint-based security door was implemented with the SM630 fingerprint scanner model and a personal computer program designed using the Visual Basic 6.0 programming language. The microcontroller (PIC16F628A) also controls the GSM modem to send 'SMS' messages when there is likely intrusion as detected through the vibrator sensor and its program was written in assembly language using MPASM VERSION 3.20 and the camera adopted the TCM321 web model. The infra-red bypass key was designed using the 555timer multi-vibrator, transistor driver circuit, the microcontroller for code generation, and set of keypad keys. The result obtained from the study showed a more reliable and trusted process to verify the authenticity of fingerprint of the door owner to gain entrance utilizing the infra- red remote-control functions to cater for any failed authentication of the registered user that might occurred. The probability of accuracy of the fingerprint security door with infrared remote-control system was 100% as against 85.71% of the existing fingerprint security door without Infrared Remote-Control system. With this assertion, it shows that the former system is compensating for the error ($\pm 14,29$) that was obtained from the later system.

Keywords: *Fingerprint security system, infra- red, remote control, door, GSM***1.0 Introduction**

Doors (wooden/metal/glass) are used to provide protection or safety to a building or place from an external intruder (Falohun *et al.*, 2012). It's ability to provide privacy and security is a factor to be considered seriously. Integrating the computer (programming skills) in controlling the opening and closing of the doors is more reliable, secured, efficient to use than that of those with handles or keys (Verma and Tripathi, 2010). In achieving these above tasks, involves the application of various

technologies, such as the fingerprint recognition technology. It is a process used to identify or authenticate an individual's identity by using their fingerprint features instead of key or passwords. The most popular biometrics technology used in automatic personal identification is the fingerprint biometric system (Maltoni *et al.*, 2005).

The reason for its popularity of fingerprint verification is that fingerprint satisfies uniqueness, stability and permanency (Khan *et al.*, 2010). Since, it offers a reliable means of personal identification, accounting for the reason it has continued to replace other methods of establishing the identities of person obstinate to admitting previous arrests. It's recognition and matching are one of simplest ways of verifying a person identity, which requires the capturing and verification of the fingerprint pattern which includes the ridges and minutia points (Gangi and Gollapudi, 2013).

One of the basic challenges with the Fingerprint Security System (FSS) is that the fingerprint of an individual can change, making identification and verification difficulty in some instances, since the system uses a high sensible fingerprint sensor to capture the fingerprints. When the fingerprint of an individual is damaged, the fingerprint patterns will be altered; thus, making authentication impossible. This problem is associated with manual or factory workers whose daily routine demands extensive use of their hands thereby resulting to cuts or bruises on the fingertips. Weakness of the finger and aging of the fingerprint template are also causal factors in the malfunction of the FSS (Falohun *et al.*, 2012). These factors can cause access denial: where an authorized user is rejected by the system. For these reasons, the fingerprint security system becomes an unpleasant biometric system and extends into some other applications resulting in the inability of a user to authenticate self, (Gangi and Gollapudi, 2013). and this can be attributed to the inability of the sensor in the fingerprint scanner to scan the damaged fingerprint (Yu *et al.* 2023). These above problems associated with the fingerprint system can be overcome with the incorporation of remote-control system (RCS) into the fingerprint biometric system, rather than discarding it completely (Ekejiuba and Folayan, 2016).

RCS technology has opened a new opportunity for improving the capacity of existing system while also upgrading the systems to ensure their maximum limit is attained (Ekejiuba and Folayan, 2016). A typical component that can implement the remote-control system capabilities is the infrared remote control. An infrared remote control that depends solely on the infrared technology, is mainly used at homes, office and to control, monitor devices quickly and easily. They are also used in analysing the different alternatives and seeking the optimal solution in each case (Gonzale and Jorba, 2013). The generated signal pulses resulted from the communication between a remote-control handset and the device

mechanism to provide actual exit. Such communication from the infrared light, is usually invisible to human eye (Lahouari, *et al.* 2007; Chen, *et al.*2021) They secure devices that are useful in peoples live and cannot be easily forged. Thus, integration of the remote-control devices was to enhance the reliability of the system and to mitigate the problem of the authentication error resulted due to the inability of the fingerprint security system to authenticate registered user.

The combination of these two technologies can result in the design of a fingerprint security door that has remote control enabled system, which enhances the system access profile and stability (Ekejiuba and Folayan, 2016). Since, the comparison of the conventional biometric methods of access (faces, Iris, fingerprint, hand geometry) and remote-control systems (RCS) devices showed that their dynamic behaviours and control operation are symmetrical in nature (Ekejiuba and Folayan, 2016). The aim of this investigation is to provide control of one or more alternative access as options to the fingerprint security door system, to enhance controllability and increase the reliability of the system (Guatam *et al*, 2013). The conclusion of this study encompasses finding solution to some the inconvenient that the registered users experiences during undergoing authentication process, using the normal system without the remote- control capabilities, such problems that are associated with biometric technologies are damaged traits, wet finger, error rates, spoofing attacks, non-universality and interoperability that can result to non-verification of the already registered fingerprint by the scanner. So, the need to utilised the infrared remote-control capabilities in providing an alternative route exit for the system cannot be overemphasized (Ekejiuba and Folayan, 2016).

2.0 Design Consideration and Analysis

The design of the circuit for the implemented system follows the block diagram of figure 1. it consist of power supply that provide power to the circuit, personal computer which is the central processing unit (CPU),

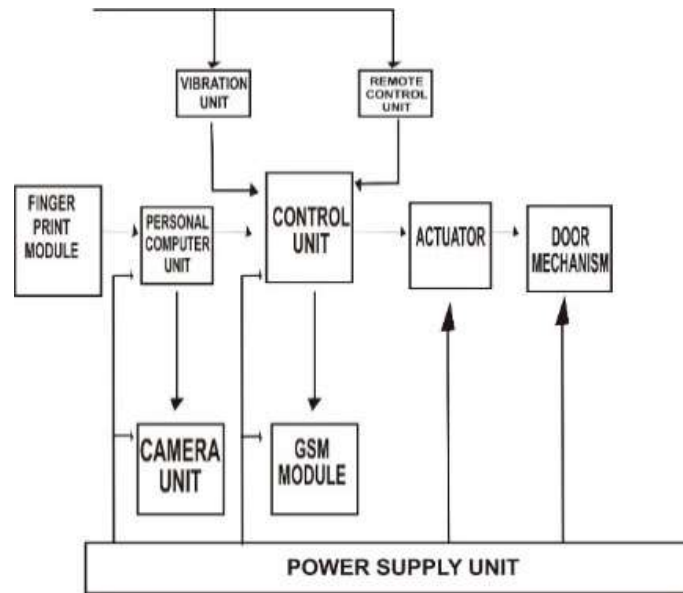


Fig 1: The Functional Block Diagram of the Design system

2.1 The Design of Power Supply

The designed system will be power-up using the alternative current (AC) and the direct current(DC) voltage sources, so that it can function accordingly. Shown in figure 2 below is the stepping down of the AC voltage to the DC voltage which is very important tasks that it performed. For the circuit to execute this task, it consists of double step- down transformer, rectifiers, and capacitors filters. The filter capacitors and the bridge rectifiers components are used for ripple voltage filtration and rectification respectively.

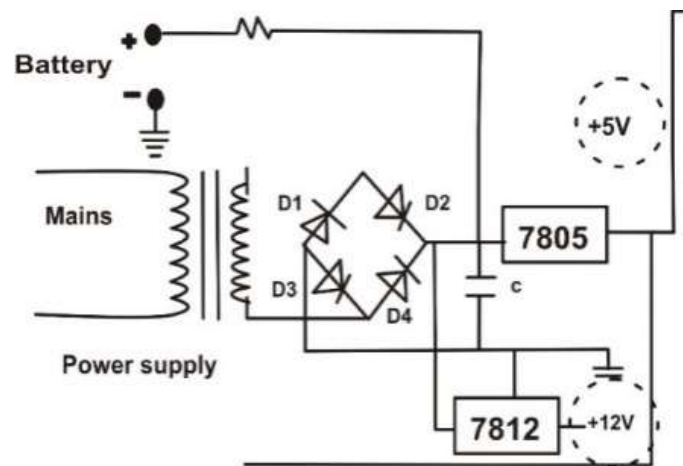


Figure 2: AC to DC Power Supply Unit

The transformer T that was used in this study has a specification of a step-down transformer of 220V to 12V ac. This transformer steps down the 220volts from the ac supply to 12 volts (Hamsa, 2015). To

achieve the required unidirectional current supply, the 12 volts AC was rectified to DC by the bridge rectifier $D_1 - D_4$. The capacitor C serve as filter capacitor (Egwaile and Oyedoh, 2019; Esenogho *et al.*, 2013)

$$\text{Peak Output Voltage } V_p = V_s \times \sqrt{2} \quad (1)$$

Where: Output Secondary Voltage $V_s = 12V$ rms

$$V_p = 16.9\text{Volts.}$$

To calculate the Peak output voltage from bridge rectifier, we used equation below:

$$V_{P.R} = V_p - 2V_d \quad (2)$$

Where $V_d = P-N$ junction drop = 0.7Volts

$$V_{P.R} = 15.5\text{Volts}$$

Capacitance Specification Used

$$\text{Ripple Voltage} = \frac{I_o}{2FC} \quad (3)$$

Where: I_o = regulator Output Current = 200Ma, V_r = Ripple Voltage = 1 Volt

$$C = \frac{I_o}{2FV_r} \quad (4)$$

$$C = 0.002 \text{ F, } C = 2000 \mu\text{F}$$

Apart from the above parameter obtained, we decided to implement the 35volts and 2200uF for the voltage and the capacitance respectively. This was considered in order to generate the needed regulated +5volts for the 7805-voltage regulator that was used in the design.

2.2 The Microcontroller Circuit

The microcontroller used in this work was the Microchip PIC16F628A (Esenogho *et al.*, 2013). It consists of 35 single cycle word instructions and two-cycle word instructions for program branches. We choose this type because of its unique asynchronous serial communication feature via RS232 protocol (Wilmshurst, 2010; Amelia *et al.*, 2017; Wang and Guo., 2009; Microchip. 2011; Esenogho *et al.*, 2013).

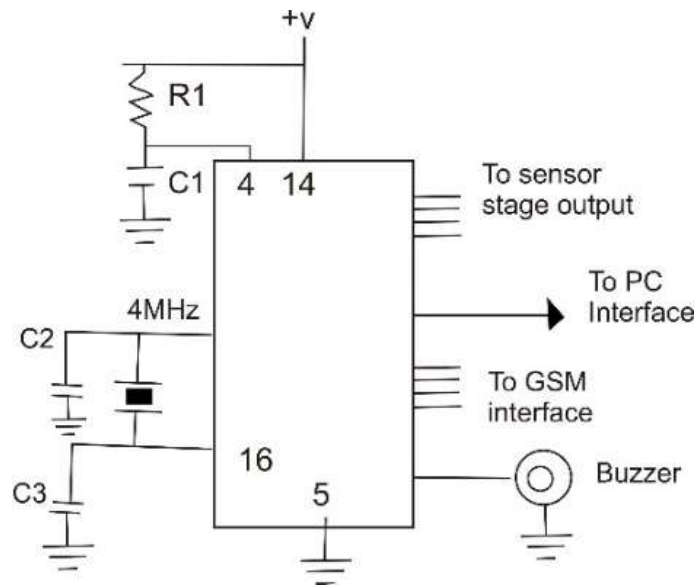


Figure 3: Microcontroller functional block circuit (Esenogho *et al.*, 2013)

2.3. Design of infra-red bypass key with infra-red transmitter and the infra-red receiver

The circuit consists of a 555 timer a stable multi -vibrator and an infra-red LED and transistor driver circuit, the microcontroller for code generation, and sets of keypad keys. It also consists of the infrared transmitter that is responsible for the infra-red-light emissions, which is a type of electromagnetic radiation with wavelengths longer than the visible light but shorter than micro waves. Shown in figure 4. below:

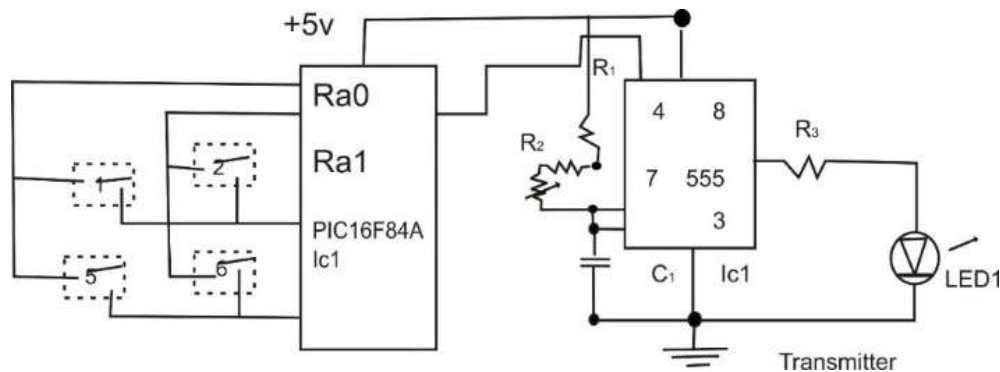


Figure 4: Key-code controller with Infra-Red Transmitter

The infra-red receiver module specially designed for infra-red reception of 38KHz signals which is infra-red receiver module IRX-TSOP 1738 model was used in the designed system. It consists of the infra-red receiver photo-diode, filter and amplification circuits and demodulator inbuilt inside it (Visbay, 2011) as shown in figure 5

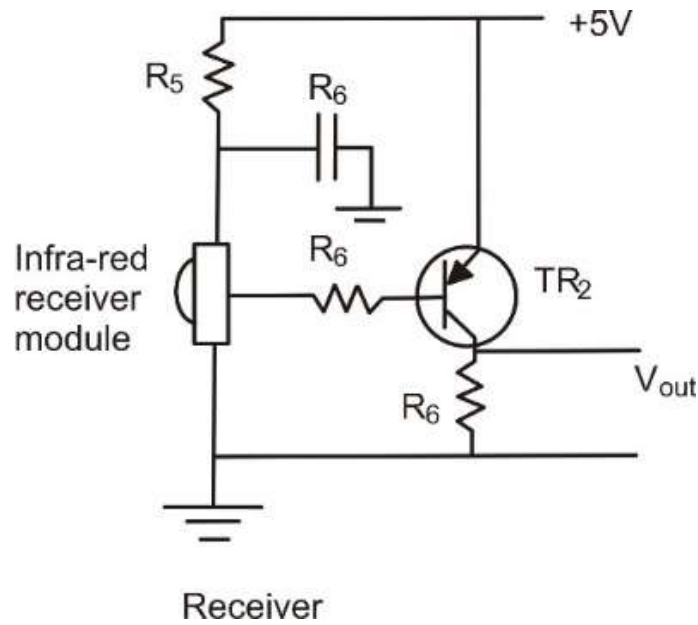


Figure 5: Infra-red Motion Detector Circuit

2.4 Design of Vibration Detector

This stage consists of the microphone sound pickup pre-amplifier. An electrets condenser microphone was used for the design and it converts sound and vibration to electrical impulses. The transistor stage provides for some signal amplification and the transistor used is the 2SC945 BJT, NPN transistor. The popular LM358 dual op-amp was used in the comparator and the preamplifier. The op-amp was used in all stages requiring an op-amp circuit in this work (Theraja and Theraja, 1999) as shown in figure 6.

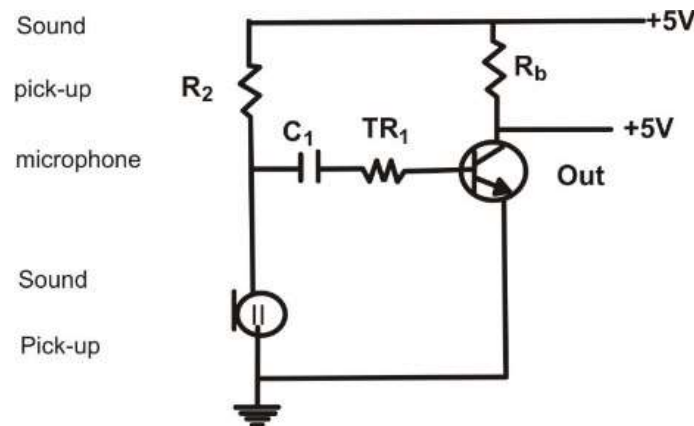


Figure 6: Schematic of the microphone and bias component

2.5 Design of Door mechanism circuit (Actuator/ Motor Drive Circuit)

The opening and closing of the door of the designed system was implemented by the motor or actuator control circuit. This circuit consists of the transistor-relay switches-controlled mechanisms, which is

powered through the DC motor which is responsible for the behavioural description of the door mechanism. The mode of operation of the two transistor relay switches circuits, involves the two transistor relay switches operations, which implies that each switch circuit is responsible for either the movement of the lock mechanism to forward direction (closing of the door) while the other moves it in the reverse direction (opening of the door). A value of $15K\Omega$ was chosen as the closest standard value (Theraja and Theraja, 1999).

2.6 Design of fingerprint Sensor/ Reader

The fingerprint sensor used is model SM63 (Okosun and Edeoghon, 2020). The sensor has four terminals for power and serial communication. The pin 1 was connected to the positive supply line from USB cable/connector while pin4 which ground was connected to ground of USB cable. Pin2 and pin3 are the sensor's Tx and Rx connected to the Rx and Tx of max232 respectively. It was used for fingerprint capture (Miaxis, 2008; Okosun and Edeoghon, 2020)

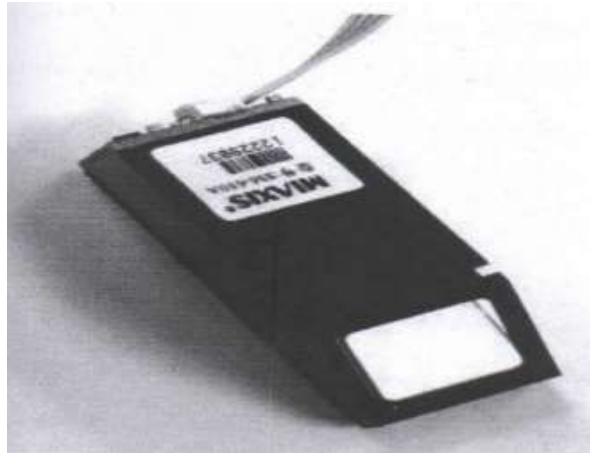


Figure 7: SM630 fingerprint reader

2.7 Design of Personal Computer Unit

The PC interfaces with the fingerprint reader module and the webcam. It checks for any fingerprint information when there is a finger placed on it and then compare the information with that in its database and if it matched. The microcontroller will receive the signal from the central processing unit (CPU) and sent it to the motor-controlled switch circuit to open the door, otherwise send a signal to the webcam to take the picture of the person at the door. The program for the PC control was designed using visual basic 6. This program was used as it is easier to understand and has very good interactive graphic user interface (GUI). The program was written such that it can register fingerprint and, also store the store information and do subsequent confirmation of any fingerprint entered after completion of the registration process.

The microcontroller program was written in assembly language using MPASM version 3.20 (Microchip, 2005).

2.8 Design of the GSM interface stage

The modem would be controlled by the microcontroller for easy communication with the MTN network. This GSM module consists of an electronic bilateral switch that interfaces with the microcontroller circuit, then the switches are directly connected to the GSM phone keys. However, many switches are necessary for the entire function of the GSM, for the querying of database and sending SMS alert (Microsoft, 2006) as shown in figure 8:

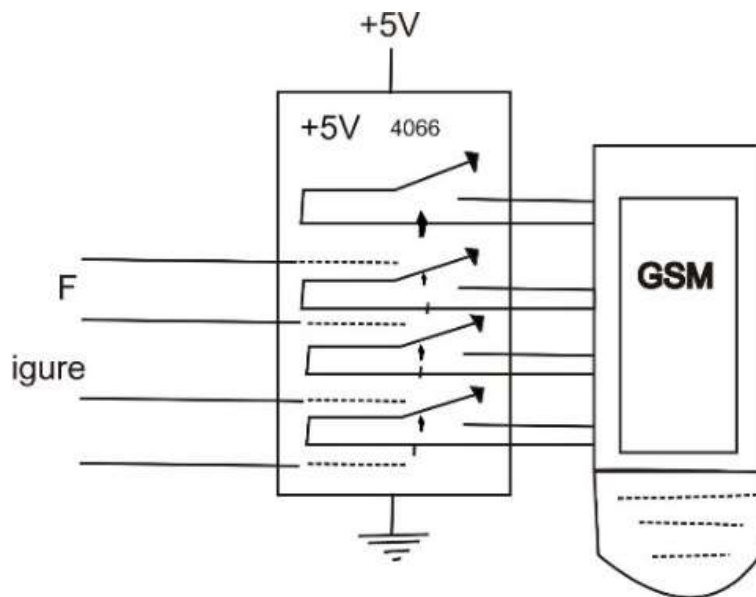


Figure 8: GSM interface Circuit

2.9 Design of web camera capture unit

The camera employed in this work is a webcam with model TCM321. The webcam was used because of cost limitation as against an analog camera with super quality and for the fact that this is a prototype unit. The camera is controlled by the PC to capture the image of the person at the door entrance and thus is saved in to the computer (Marijana, 2004; Hamsa, 2015).

2.10 Database design

The database for biometric security door system was done using the Microsoft Access 2007 edition. The fields created include username, date, time of access and ID. The software that was used to run the program is the Microsoft visual basic 6 professional edition. The visual basic application was interfaced with the database using the Active X Data Object (ADO) data control, which is embedded in the visual

basic program in its active X module. This module Microsoft ADO Data Control can be selected from the component section of the visual basic 6 toolbox and is added to the toolbox (Microsoft, 2006).

The database design was done using a table representing those users to be registered using the biometric sensor as presented in tables 1, that shows all the records of persons that were registered into the system with their name, sex, biometric ID, address, department, email, date time, and the corresponding headings as in serial number, name, description, data type, and field size.

Table1: Result sheet of registrations into the system

S/No	Name	Description	Data Type	Field Size
1	Name	Full names of person being registered or already registered	Text	50
2	Sex	Gender of person	Text	2
3	ID	ID number	Numeric	5
4	Address	Address or contact of the person	Text	50
5	Department	Department of the person	Text	50
6	Email	Email address of the person	Text	50
7	Date	Date of registration or access	Date	10
8	Time	Time of access	Time	12

The visual basic 6 program was used to create the graphic user interface to interface to the database and generate the record for display. The GUI controls include; Username, Time, ID, Date and control buttons for; Register, Identify, Delete, Open, Close, Clear all, Exit and Admin Key. Figure 9 shows the database created from the Microsoft Access 2003. It shows all the fields.



Figure 9: Database created with Microsoft Access 2007.

The visual basic program was then created with the ADO module and its connection string was referenced to the database and the code was then written to access the database. The visual basic program served as the software interface to the database. As shown in figure 10 below:

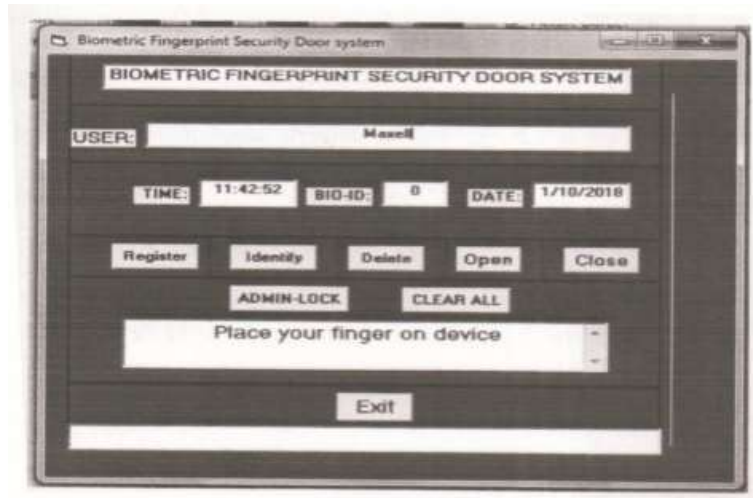


Figure 10: Graphic User Interface (GUI) to the database

2.11 Casing and Software Security Design

2.11.1 Casing

In designing the hardware enclosure (casing), we used materials like ABS plastic for durability, security and aesthetic appeal. The compact enclosure fits neatly on the door, protecting internal components while allowing easy access to the fingerprint sensor and IR receiver. It was easily mounted on the door, with secured fasteners, and minimal exposed screws. We also provided ventilation slots to prevent over heating of the internal components. We ensure that the designed system integrate smoothly with the door's locking mechanism, ensuring alignment and secure mounting. As shown in figure 11 below;



Figure 11: Casing (enclosure) of the Designed System.

2.11.2 Software Security Designing

We ensured that the data generated was secured, which implies that each fingerprint data, IR commands, and other communication between components are encrypted, to prevent unauthorized access., securing critical components (like microcontroller, power supply) inside the enclosure to prevent physical attacks.

The multiple layers of authentication were implemented, such as requiring both fingerprint and IR compared for access and finally included features like audit trails, alerts for attempts or unusual activity.

2.13. Prototyping

A prototype system was built, using the designed PCB and components, placing everything inside a preliminary enclosure (Casing). All individual modules (fingerprint sensor, IR remote, lock mechanism) were tested to ensure they are functioning correctly and interact smoothly. In turns, all the modules were integrated and the full designed prototype system is shown in figure 12 was also tested ensuring that the fingerprint authentication and the IR remote control are working together without and any stress.

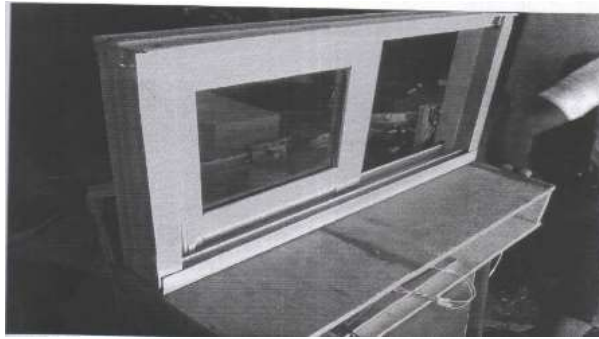


Figure 12: Prototype designed full biometric fingerprint security door with infra- red remote control and GSM alert system.

2.14. Full circuit diagram of the designed system

Figure 13 shows the complete circuit diagram of the fingerprint security system with infra-red remote control and GSM alert system. It consists of the hardwired construction and the software development. In the hardwired contribution stage, we designed a stable power supply circuit that provides the required voltages for all the components. That can stepdown 220v to 12volt. The microcontroller (microchip PIC16F628A) serves as the central processing unit. It was connected to all the input components (the SM630 fingerprint scanner, IR receiver) and the output devices such as the (door lock, LEDs). The transmitter (Tx) and the receiver (Rx) pins of the fingerprint scanner was connected to that microcontroller's Tx and Rx pins respectively, for serial communications and was powered using 5volt. The IR receiver's output pin was connected to one of the microcontroller's digital input pins and which was powered using the 5volts that has a direct line of sight to the Infrared remote control.

The relay's control pin was connected to a digital output pin on the microcontroller, which in turns controlled the door lock mechanism via the motor or actuator control circuit, which is responsible for the opening and closing of the door, depending on the signal obtained. A diode was connected across the relay coil to prevent back EMF from damaging the microcontroller. Then the LEDs was connected to the

microcontroller's output pins for status indication (to show fingerprint accepted, access granted, access denied). The vibration sensor's output was connected to the digital input pin on the microcontroller, in order to enable it to trigger an alarm or send an alert, if tampering is detected. The GSM module was connected to the microcontroller via serial communication (Tx/ Rx pins) to enable us to use the module to send SMS alerts or receive remote commands.

Lastly, the camera module was interfaced with the microcontroller for capturing images during the access attempts. All these connections are shown in figure 14a and 14b respectively. The visual basic program was developed to respond the fingerprint device for registration, confirmation, identification and verification procedures to help with the interactive requirements between the user and the fingerprint machine (Annie *et al*, 2014). Then for the software development stage, this commenced with the programming of the microcontroller to carry out the below functions:

- (i) The fingerprint Authentication: a firmware to interface with the fingerprint scanner was written to carried out its essential functions which includes enrolling fingerprint, storing them, and authenticating users.
- (ii) The microcontroller was programmed to decode IR signals from the remote and trigger the appropriate action (locking / unlocking the door).
- (iii) The microcontroller was also programmed to implement the logic for locking / unlocking door based on fingerprint authentication or IR remote commands.
- (iv) Efforts were made to ensure that the system can fallback IR remote control if the fingerprint authentication fails.
- (v) Codes were developed for handling vibration sensor inputs, sending SMS alerts via GSM module, and capturing images with the camera module.

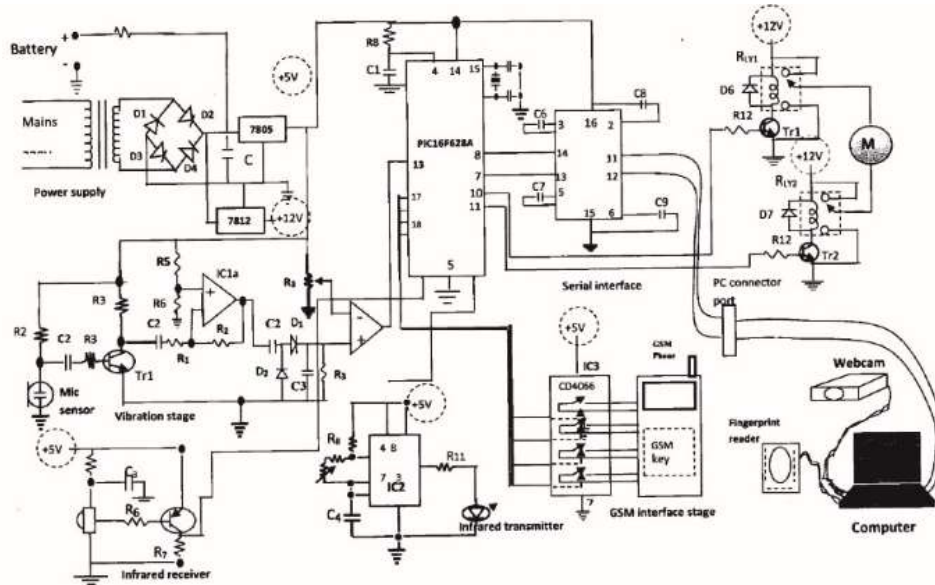


Figure 13: Complete diagram of the fingerprint security door with infra- red remote control and GSM alert system.

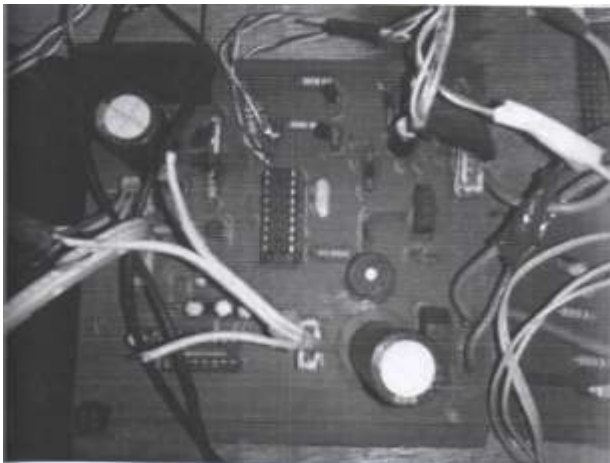


Figure 14a: Partly Completed design of the circuit



Figure 14b Partly Completed design of the circuit

2.15 Design of Fallback Logic Implementation unit

(a). Fingerprint Failure Handling:

- i. Set a maximum number of fingerprint attempts (e.g., 3).
- ii. If fingerprint authentication fails, signal the user to use the IR remote (e.g., flashing LED).
- iii. Allow the IR remote to unlock the door after fingerprint failure.

(b). Fallback Mode Activation:

- iv. If fingerprint fails, activate the fallback mode where the system listens for IR remote commands.

- v. A valid IR unlock command will unlock the door; otherwise, the door remains locked.

2.16.1 Software Workflow

The software workflow for the machine was presented as a pseudocode as shown below while the flowchart is shown in Figure 15.

Start

```

initialize system () {
  setup_fingerprint_sensor ()
  setup_IR_receiver ()
  setup_feedback_devices ()
  setup lock ()
}
while (true) {
  if (fingerprint_scanned ())
    if (authenticate_fingerprint ())
      unlock_door ()
      reset_failure_counter ()
    }
  Else {
    increment_failure_counter ()
    if (failure_counter >= MAX_ATTEMPTS)
      activate_fallback_mode ()
  }

  if (fallback_mode_active) {
    if (IR_command_received ())
      if (validate_IR_command (IR_UNLOCK_COMMAND))
        unlock_door ()
        reset_failure_counter ()
        deactivate_fallback_mode ()
      provide_user_feedback ()
      sleep ()
  }
}

```

Stop

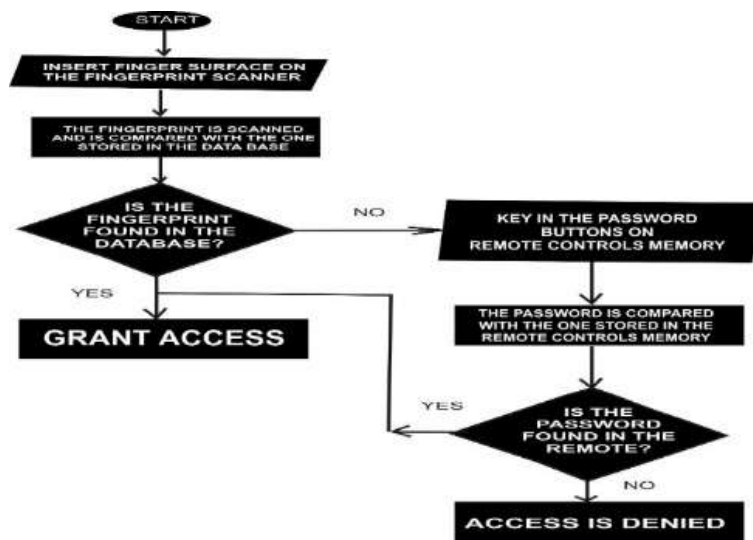


Figure 15: Flowchart of the remote control and fingerprint authentication system

3.0 Testing and Results

The University of Benin, computer Engineering staffs was used as a case study. Four (4) staffs were enrolled participated using the fingerprint biometric sensor. They were enrolled for their fingerprint template registration and verification; hence the designed system displays a status, “successful” if their fingerprints were registries and verified. In carrying out these tasks, a series of tests were carried out using the designed system its biometric sensor, and various results were obtained, which shows the expected response of the biometric sensor of the fingerprint security door system and was successful and satisfactory. The result is presented in figure 16 shown below:





NAMES OF PERSONEL	FINGER PRINT RESULTS		COMMENT
OKOYE JAMES		Successful	Satisfactory
EGUAGIE EBVOMWAN		Successful	Satisfactory
UGOCHI PETERS		Successful	Satisfactory
EMEKA EJOFOR		Successful	Satisfactory

Figure 16: Test results of the security device with biometric sensor

3.1 Real- Time Deployment Test Results

The University of Benin, computer Engineering 400 level class was used as a case study. Seventy (70) students participated. In carrying out these tasks, two systems were involved, the designed fingerprint security system with the IR remote-control capabilities and the one without. The fingerprint security door system without infra-red remote controls system was used to collect fingerprints images from seventy (70) students for registration purposes, but the system registered all the seventy (70) students, but during authentication process, we discovered that ten (10) students were unsuccessful. On the other hand, the developed fingerprint security door with infrared remote-control system showed 100% successful rate of tested individuals.

From the above analysis, the value of the Unsuccessful authentication (FA) was nil, because the remote control was used to normalize the authentication error, resulted from the biometric angle of the developed system. The developed fingerprint security door with infrared remote-control system was compared with the one without the remote control, and the number of authentications was recorded. Observations

showed that the latter recorded ten (10) individuals that experienced false authentication as against none for the former, as shown in table 1:

Table 1: Details of the Comparison of the two system.

Type of System	No of individuals	
	False Authentication	Truth Authentication
Fingerprint Security door with Remote Control System	0	70
Fingerprint Security door without Remote Control system	10	60

3.2 Accuracy Testing

Given a fingerprint matcher, as the fingerprint security door with infra-red remote control and GSM alert, the need to assess its accuracy as against existing system, which its fingerprint scanner sometimes some degree of uncertainty that normally result to inaccuracy computation. The uncertainty matching leads to false authentication (FA) and the exact matching is known as the Truth authentication (TA). So, to ascertain how accurate the designed system in performing the expected task in a real- time basis was done. In doing so, their probabilities were computed and compared to obtain the accuracy of both systems.

3.2.1 False Authentication (FA)

The probability of this happening is referred to as the False Authentication Ratio (FAR). FAR is defined by the formula:

$$F.A.R = \frac{\text{Number of F.A. that occurred}}{\text{Total Number of F.A. that occurred}} \times 100\%$$

$$FAR = \frac{FA}{N} \times 100 \quad (5)$$

3.2.2. Truth Authentication (TA)

The probability of this happening is referred to as the Truth Authentication Ratio (TAR). TAR is defined by the formula.

$$T.A.R = \frac{\text{Number of T.A. that occurred}}{\text{Total Number of T.A. that occurred}} \times 100\%$$

$$TAR = \frac{TA}{N} \times 100 \quad (6)$$

Therefore, using the above equation (5) and (6) respectively, Then, their respective values for the False Authentication Rate (FAR) and Truth Authentication Rate (TAR) were 14.29% and 85.71% respectively.

it is then evident that the values for FAR and TAR, implies that the accuracy of the fingerprint security door with infrared remote-control system was 100% as against 85.71% of the existing fingerprint security door without Infrared Remote-Control system. With this assertion, it shows former system is compensating for the error (+_14,29) that was obtained from the latter system.

4.1 Conclusion

This study solves the problems generated by the fingerprint security door system without the remote-control capabilities, such as damaged fingerprint that could cause poor identification and verification of individuals registered in the system, the aim of providing control of one or more alternative access as option to the fingerprint security door system, in order to enhance controllability and increase reliability of the system has been addressed, with the successfully incorporation of the infrared remote-control capabilities into the existing system functionalities as showed in this study.

REFERENCES

- Afritha Amelia, Julham, Bakti Viyata Sundswa, Mortlan Parclede, Wiwinta Sumiao and Muhammed Rusdi (2017) Implementation of the RS232 communication trainer using computer and the ATMEGA microcontroller for interface engineering courses. IOP conf. series, Journal of physics: cont. series 890 (2017) 012095. IOP Publishing Doi: 10.1088/1742-6596/890/1/012095.
- Angel Gonzalez Villian, and Josep Jorba (2013) Remote Control Mobile Devices in Android Platform. arxiv: 1310.5850v1 [CS.HC } 22 oct 2013. <https://www.researchgatenet.publication>.
- Annie O. P, Rahul A. P, Pranav V, Ponni S, Renjith N (2014). Design and Implementation of a Digital Code Lock. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)*, vol. 3, no. 2, pp. 7604-7607, 2014. February 2014 ISSN (print): 2320-3765, ISSN (online) 2278 – 8875.
- Chen, Yuanyi (2021). Research on Application System of Remote-Control Computer of Android Mobile Phone. *Journal of Physics Conference Series*. 1992.022169.10..1088/1742-6596/1992/2/022169. Pages 022-109.
- Ebenezer Esenogho, Neville Idiagi, Igimoh, John (2013). Development and Implementation of a Biometric Security Lock system. Journal of Nigeria Association of production Engineers NIPRO DE. March 2013. Pp. 121-133. Citation- 270272469.bib
- Egwaile, J.O., and Oyedoh, M (2019). Design and Construction of a Programmable Password Operated Circuit Breaker. Journal of science and Technology Research 1(1) 2019 pp206- 220. Journal homepage: [www. NIPES Journals. Org](http://www.NIPESJournals.Org) ng.
- Ekejiuba C. O and Folayan G. B (2016), Remote Controlled Security Door. *Journal Electrical Electronic System*, 5:2 184. DOI: 10.4172/2332-0796.1000184. ISSN-2332-0796.

- Falohun, A.S, Omidiora E, O, Fakolujo O.A, Afolabi A, O, and Oke A.O (2012): Development of a Biometrically-Controlled Door System (using IRIS) with Power Back up: American Journal of Scientific and Industrial Research. Vol. 3, No 4, pp203-207, ISSN2153- 649X, Science Hub Publications, U.S.
- Gangi, R.R., and Gollapudi, S, S, (2013).; Locker Opening and Closing System. *International Journal of Engineering Trend & Technology in Computer Science (JETTCS)*
- Gautam L, Sharma C, Arora A, Pinku Yadav (2013). Developing Infrared Controlled Automated Door System. *International Journal of Modern Engineering Research (IJMER)*, Vol. 3, Issue. 5, Sep - Oct. 2013 pp-2872-2874 ISSN: 2249-6645
- Hamsa F. T, (2015). Safety and Security of the Personal Belongings Using Microcontroller. *Diyala Journal of Engineering Sciences*, vol. 8, no. 2, pp. 28-37, 2015.
- Khan B., Khan M. K. and Alghathbar K.S (2010); Biometrics and Identity Management for Homeland Security Applications in Saudi Arabia. *African journal of Business Management Vol. 4(15)*, pp. 3296-3306, 4 November, 2010. <http://www.academicjournals.org/AJBM> ISSN: 1993 – 8233 @2010. Academic Journals.
- Lahouari Kaddour-El Bouadi, Jean Vareille, Philippe Le Pare and NasreddineBerrached (2007). Remote control on internet, long distance experiment of remote practice works, measurements and results. Published in *international Review on Computers and Software* 23 (2007) 206 – 216.
- Maltoni D., Dario Maio, Anil K. Jain, Salil Prabhakar (2005). *Handbook of Fingerprint Recognition - Second Edition Springer, London, 2009*. Published in springer professional. 10 march (2005) Computer Springer Professional Computing. Doi: 10.1007/597303. <https://api.semanticscholar.org/corpusid:8709950>.
- Marijana, K (2004). Passport of the future: Biometrics against Identity Theft. M.Sc. thesis in Information security. Norwegian Information Security Laboratory (NISlab) (<https://apc.semanticscholar.org/corpusID:114146979>). @inproceedings{Kosmer1J2004passportOT}.
- Miaxis Biometrics Co. Ltd (2008). SM630 Fingerprint Verification Module User Manual (pdf).
- Microchip (2005). MPASM Assembler, MPLINK Obect Linker, MPLIBMPLIB Object Librarian User Manual (pdf).
- Microchip (2011). PIC16F627A/ PIC16F628A/ PIC16F648A Datasheet: FLASH-Based 8-bit Microcontrollers
- Microsoft Access 2003 Resource Centre (2006). Current Method [Access 2003 VBA language Reference] [www.microsoft.com/C/ Current Method \[Access 2003 VBA language Reference\]](http://www.microsoft.com/C/CurrentMethod)
- Microsoft Visual Basic 6.0 Resource Centre (2005). Visual Basic 6.0 Documentation. [www.microsoft.com/VisualStudio/Visual Basic 6.0](http://www.microsoft.com/VisualStudio/VisualBasic6.0)
- Okusun, O. And Edeoghon, A.I (2020). Design and Construction of a Wireless Fingerprint Attendance Management System Based on Zigbee Technology. *Journal of Civil and Environmental Systems Engineering*. Vol 18, ISSUE 1, July 2020. Pages: 92- 99. ISSN- 15965538.

- Theraja B.L. and Theraja A.K (1999). /*A Textbook of Electrical Technology in SI units, Vol 1 (1st Edition) Basic Electrical Engineering of Origin. Paper Back, 734 pages, published 1999 by S CHAND and CO ISBN-13: 978-81-219-0290-8, ISBN: 81-219-0290-8
- Tim Wilmshurst (2010). Designing Embedded Systems with PC Microcontrollers- (Principles and Applications). Published by Elsevier Ltd. Pp 295- 337. [https://doi.org /10. 1016/ B978-1-85617-7504. 10013-7](https://doi.org/10.1016/B978-1-85617-7504.10013-7). All right reserved. Copy right @290 Tim.Wilmshurst.
- Verma, G. K., & Tripathi, P (2010). A digital security system with door lock system using RFID technology. *International Journal of Computer Applications*, 5(11), 6-8. P. P (0975-8887) Doi = (10.5120/957-1334), <https://reasarchgate.net/publication/45602075>.
- Vishay Siliconix (2011). TSOP1738, photo modules for PCM Remote control system. 204.66 kbytes, 7 pages, <https://www.alldatACom/datasheet-pdf/26589/VISHAY/TSOP1738.html>. <http://www.vishay.com>.
- Xianjun Wang, Wencheng Guo. The Design of Rs232 and CAN protocol computer based on Pic, MCU. *Journals of Computer and Information Science*. Vol. 2, No. 3 (2009). Doi: 10.5539/Cis. V2n3p176. Creative Commons Attribution 4.0 license. ISSN (Online) 1913 – 8997. ISSN (Print) 1913 – 8889 (Wang and GUO., (2009).
- Yirong Yu., Qiming Niu,m Xuyang Li., Junshe Xue., Weigues Liu., and Dabin Lin, (2023).; Review of Fingerprint Sensors: Mechanism, Characteristics, and Applications. *Journal of Micromachines*. Volume 14, issue 6, 1253; <https://doi.org/10.3390/mi14061253>, 14 June 2023. MEMS/NEMS Sensors and Actuators, 2nd Edition.