[1.]Tertsegha Daniel IPILAKYAA, [2.]Victor OJI, [3.]Vincent OKEKE

DESIGN, CONSTRUCTION AND PERFORMANCE EVALUATION OF AN AUTOMATED DOOR LOCK USING BIOMETRIC SECURITY SYSTEM WITH PHONE TEXT ALERT NOTIFICATION

[1-3.]Department of Mechanical Engineering, Federal University of Agriculture, Makurdi, Benue State, NIGERIA

Abstract: The design, construction and performance evaluation of an automated door lock using a biometric security system with phone text alert notification which helps in notifying the owner of an intruder have been carried out. A fingerprint sensor, Subscriber Identity Module (SIM), Liquid-Crystal Display (LCD) screen and an Arduino Uno board microcontroller were used for the design. The fingerprints of authorized persons are stored on the microcontroller memory using a keypad for input. By using a matching algorithm, the microcontroller for every finger placed on the print checks if the print is registered on its database. If registered, it displays a welcome message on the LCD screen. For unauthorized/unregistered person, the microcontroller will deny access, at the same time send a text message to a secured and registered Subscriber Identity Module (SIM) card about an ongoing home break. This causes the receiver to initiate any counter measures needed. The design helps to provide high quality security on doors at a minimal cost.

Keywords: Microcontroller, Fingerprint Sensor, LCD Screen, SIM card module and Locking Mechanism

1. INTRODUCTION

Technological advancement has been on the rise since the past 2 centuries. Due to the rise of the rate of technological advancements, measures have to be taken to protect tangible assets that can be looted resulting in high expenses to the owner(s). When it comes to security systems, it is one of the primary concerns in this busy competitive world, where human cannot find ways to provide security to his/her confidential belongings manually. Instead, he/she finds an alternative solution which provides better, reliable and atomized security.

The technological advancement has evolved to a point where everything is connected thus making information secure as well as volatile thus resulting in the outlook for complexity of security measures [1]. Due to the insecurity as a result of the technical advancement, measures are taken to safeguard the necessary assets that are vital.

Many security systems including passwords, pins and even as simple as keys may be efficient means in a way but have their deficiencies. A power surge of the right current can damage the circuits thus causing it to malfunction and any computer professional can hack into passwords or pins and gain access. Keys are not configured to just a single person therefore once anybody else gets the keys, such a person automatically gets access to the door being locked. Hence the use of biometrics is seen as the next most proficient means of security.

The system here is being programmed to the fingerprints of the single or multiple users as the case may be in a home and can only be opened by the user(s) since no two fingerprints are identical. This design is implemented to provide better securities as users don't need to remember passwords and don't need any sort of keys or cards that often get lost. If someone's fingerprint is authorized in the system he/she would not face any sort of delays to enter a room.

ANNALS of Faculty Engineering Hunedoara – International Journal of Engineering
ISSN 1584 - 2665 (printed version); ISSN 2601 - 2332 (online); ISSN-L 1584 - 2665
Universitatea Politehnica Timişoara

Fingerprint recognition is one of the most secure systems because a fingerprint of one person never matches with others. Therefore, unauthorized access can be restricted by designing a lock that stores the fingerprints of one or more authorized users and unlock the system when a match is found. Bio-metrics authorization proves to be one of the best traits because the skin on our palms and soles exhibits a flow like pattern of ridges on each fingertip which is unique and immutable. This makes fingerprint a unique identification for everyone. The popularity and reliability on fingerprint scanner can be easily guessed from its use in recent hand-held devices like mobile phones and laptops [1].

2. LITERATURE REVIEW

Several works on lock systems have been done using different methods to grant or deny access to doors. Fingerprint scanner was used as the medium of access. Fingerprint enrollment was done for the authorized user. The pattern of the thumb and index finger was scanned and stored in the system. To gain access, the fingerprint of the user must match the pattern thumb and index finger. If a wrong fingerprint is detected for three consecutive times, the system automatically generates a passcode which it sends to the mobile phone of the authorized user to alert him of the intrusion [2]. Password system was used in to authenticate the user, a numeric code of four digits entered and the microcontroller checks to see if it matches with the preset password. If it matches, the locker is opened, if not buzzer is activated and it sound an alarm [3].

The use of fingerprint for identification has been employed in law enforcement for about a century now [4]. A fingerprint lock system using microcontroller uses fingerprint recognition system as a process of verifying the fingerprint image to open the electronic lock. This research highlights the development of fingerprint verification system using Arduino 1.6.3. Verification is completed by comparing the data of authorized fingerprint image with incoming fingerprint image. The incoming fingerprint image will first go through the extraction and filtering processes through which the information about it is obtained. Then the information of incoming fingerprint image will undergo the comparison process to compare it with authorized fingerprint image. In this work, the fingerprint module was trained to learn and identify whether the incoming fingerprint image is genuine or forgery. A much broader application of fingerprint is for personal authentication, for instance to access a computer, a network, an ATM-machine, a car or a home.

Cortez et. al., developed a locker system based on biometric and short message service technologies. The study made use of biometric technology for data enrolment, and short message service for passcode generation and authentication [2]. Patil ad Reddy developed an office automation system using Radio Frequency Identification (RFID) and GSM technology [5, 6]. This study made use of both RFID and GSM technology to electronically control the opening and closing of doors.

3. MATERIALS AND METHODS

The microcontroller (ATmega328) which has a 16 MHz crystal oscillator was used. A fingerprint sensor for accepting and accessing placed prints was a vital component. For the notification, a SIM800L GPRS GSM module Micro SIM Card Core Quad-band TTL Serial Port Antenna PCB Wireless WIFI Board for Arduino smart phone was used with an MTN SIM as the source for notification. For the power supply, a 12v DC adaptor was used to power the entire circuit. A retractable solenoid was used for the locking mechanism.

Hardware used:

- ATmega328/Arduino Uno
- Fingerprint sensor (AS608)
- SIM card module (SIM800L)
- Liquid Crystal Display (HD44780 16×2 IIC character)
- Locking mechanism

ATmega328/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 crystal oscillator, 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 an AC-to-DC adapter or battery to get started. The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega8U2 programmed as a USB-to-serial converter [7].

The recommended supply voltage is 7-12V while the operating voltage is 5V. The DC current per I/O pin is 40 mA while the DC current for 3.3V pin is 50mA. The flash memory is 32KB of which 0.5 KB is used by the bootloader. The SRAM of the device is 2 KB while the EEPROM is 1KB with a clock speed of 16 MHz.

—**Fingerprint Sensor**

A fingerprint is an impression left by the friction ridges if a human finger. A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. It has the following specification:

- Supply voltage: 3.6 - 6.0VDC
- Operating current: 120mA max
- Peak current: 150mA max
- Fingerprint imaging time:<1.0 seconds
- Window area: 14mm x 18mm
- Signature file: 256 bytes
- Template file: 512 bytes
- Storage capacity: 162 templates
- Safety ratings (1-5 low to high safety)
- False Acceptance Rate:<0.001% (security level 3)
- False Reject Rate:<1.0% (Security level 3)
- Interface: TTL Serial
- Band rate: 9600, 19200, 28800, 38400, 57600 (default is 57600)
- Working temperature rating: -20C to +50C

—**SIM Card Module**

The Subscriber Identity/Identification Module (SIM) widely known as a SIM card is an integrated circuit that is intended to securely store the International Mobile Subscriber Identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices as well as to store contact information. This is the component that sends a notification SMS to a secured line about an unauthorized entry. The module receives power from the Arduino Uno board via a 1N4001 diode. It has four wires of which one is for the found connection, one powers the component with specifically 5V and the other two transmit data.

—**Liquid Crystal Display**

The Liquid Crystal Display (LCD) is a flat display used to output text and other ASCII symbols to the user. The LCD screen built specifically for the Arduino usually come in as a 16x2 display. That is, the character limit is 16 in width and 2 characters in height. That is 16 columns and 2 rows of letters, numbers, or symbols resulting in a total of 32 characters. Each character has 40 pixels. For 32 characters, the total number of pixels will be (32×40) 1280 pixels.

—**Locking Mechanism**

An electronic door-lock solenoid (connected across connector CON3) is basically an electromagnet made of a big coil of copper wire with an armature (slug of metal) in the middle. When the coil is energized, the slug is pulled into the center of the coil. This allows the solenoid to move to one end.

—**KEYPAD**

The keypad is another fundamental component of the setup. Its main function is to register a fingerprint and also to erase an old fingerprint. It's a 4×4 keypad connected to the Arduino Uno board via pins to allow the user input and register his fingerprint unto the microcontroller while the LCD serves as an interface telling the user what to do at a particular point in time.

—**BLOCK DIAGRAM**

The block diagram of the entire system is shown Figure 1. The Arduino Uno being the most vital component, coordinates every action of both the software and hardware components. All other components linked to the Arduino are to be regulated based on the various inputs signals given to the system.

The microcontroller is located in the middle of the entire setup while other components that act and transmitters and/or receivers of data are connected to it for the effective operation of the entire system.

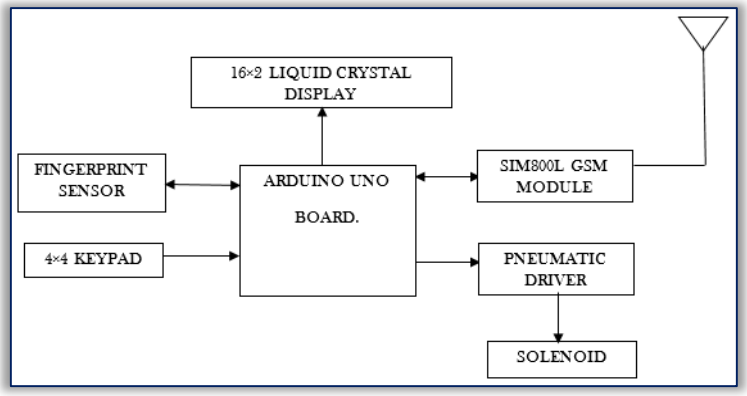

Figure 1: Block Diagram of an Automatic Door Lock Using Biometric Security System

—SOFTWARE DESIGN AND EXECUTION METHODOLOGY

The design of the software and its operation is seen in the flowchart shown in Figure 2 while the software program is shown in Figure 3.

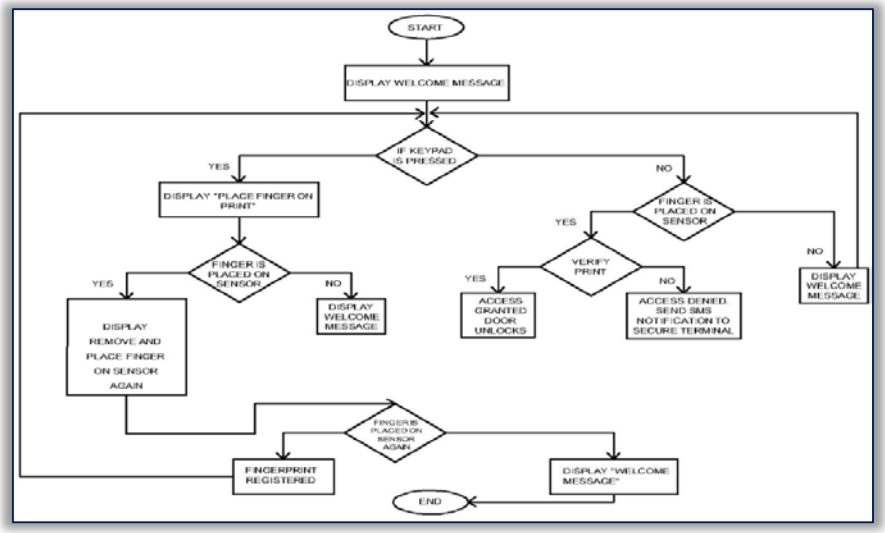

Figure 2: Flow Chart Showing the Software Design and Execution Process

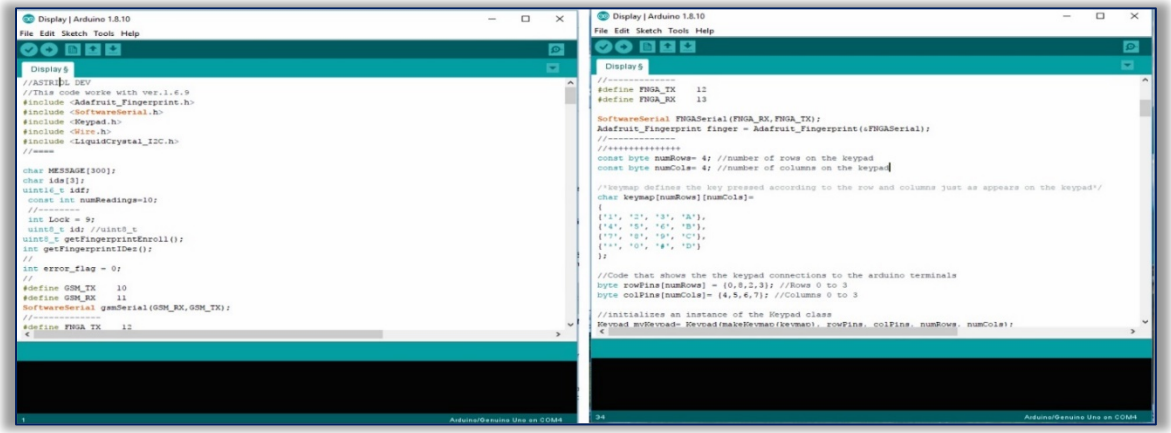

Figure 3: Shows a software program

—Mode of Operation

Figure 1 and Figure 2 give us a detailed outlook on the entire operation in both the alignment of the hardware and the software regulating the operation of the hardware. When the system is powered on, the sensor becomes active; the first step for a new system is the registration. A variable is always allocated to every fingerprint ranging from 0-9. The key * is pressed to allow the input for a new fingerprint and the desired variable. The finger is placed on the sensor and removed once it has been captured. It is placed again on the sensor and the print is officially registered. Once this condition is met, the person now has access.

For the opening of the door, the keypad needs not to be pressed as can be seen in the flow chart. Once a finger is placed on the sensor, the microcontroller tries to verify the print by matching the current print with the various print(s) stored in its memory. Once the verification process is complete and a match is found, the person gains access and the door opens while displaying a welcome message on the LCD. However, if there is no match, the person is denied access and automatically, the SIM card module sends a notification message to a secured end of an intrusion.

4. RESULTS AND DISCUSSION

The program for the Arduino Uno microcontroller was written in C language as shown Figure 3 and was then compiled into an executable file using the Arduino IDE. The circuit as shown in Figures 4a and 4b was designed on the bread board. The code already written on the Arduino IDE was compiled and uploaded to the microcontroller.

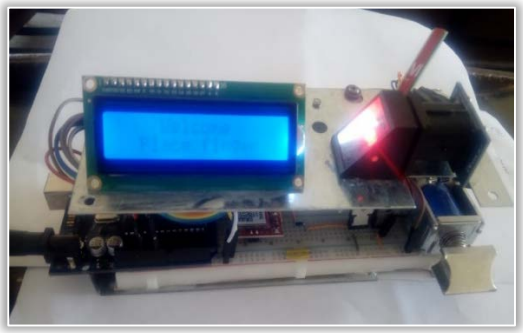

Figure 4a: Designed project on board without keypad for fingerprint registration

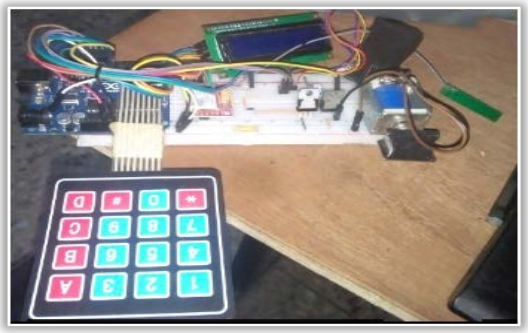

Figure 4b: Designed project on a bread board with the keypad for registration of fingerprint

Figure 5 shows the welcome message to whoever is at the point of entry. It is a perpetually occurring message as long as there is power supply. Figure 6 shows the shows the notice of placement of fingerprint. At the same instant, the fingerprint sensor comes alive and is ready to receive any finger.

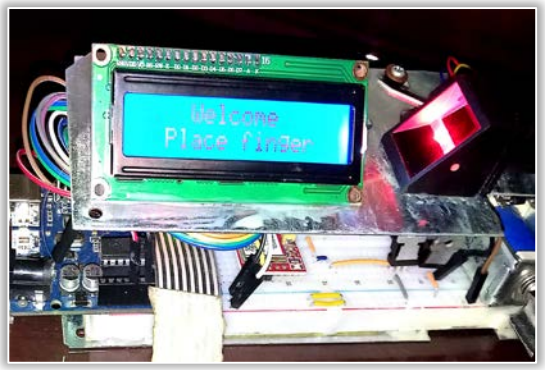

Figure 5: Display of welcome message

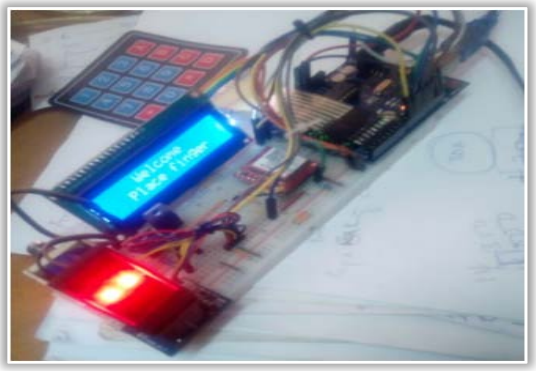

Figure 6: Showing fingerprint sensor ready to read print and message on screen

Figure 7: Welcome message to user with recognized print

Figure 7 shows that the user has clearance and is allowed to enter as it displays access granted. Figures 8 and 9 shows that the user has no clearance and is not allowed to enter. It displays the access denied phrase and automatically sends an SMS as shown in Figure 9.

Figure 10 shows the secure line which receives the notification of a break-in.

Figure 8: Message showing an intruder trying to gain access

Figure 9: message showing that an sms has been sent

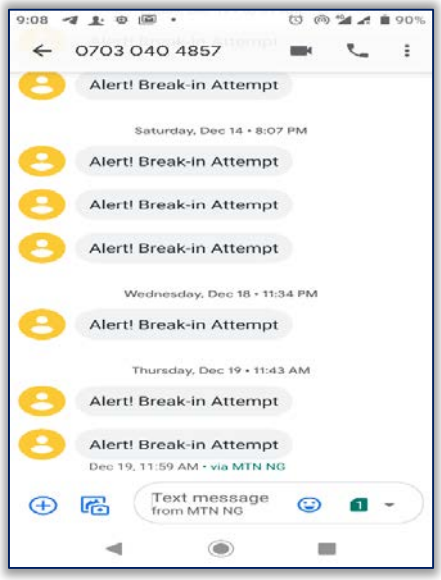

Figure 10: message showing that an SMS has been received

5. CONCLUSIONS

The fingerprint-based security door control system development in this study enables door to be electronically operated. It eliminates the challenges attributed to reliance on human security. It requires little or no human intervention in opening and closing the door; thus, a greater level of security and efficiency. The performance of this system in terms of time to recognize user has made it more effective as compared to other existing system. In order to maintain security properly, the whole mechanism should be placed inside the door panel or on the other side of the door. A system for batteries could also be made or even solar powered. Several other systems can be implemented with this system. The system is very secure. It provides greater control for access to restricted places. It is worth noting that the system needs high power to operate so providing continuous power through batteries is a challenge sometimes. A power failure will make it unworkable. In that case, we can, connect the system with an Integrated Power System (IPS) or add rechargeable batteries to the system.

References

[1] Odiete, J. O.; Agbeyangi. A. O.; Olatinwo O.: An Automated Door Control System using Biometric Technology. IOSR Journal of Computer Engineering (IOSR-JCE). Vol. 19, Issue 4. pp. 20-25, 2017.
[2] Cortez, C.D.; Badwal, J.S.; Hipolito, J.R.; Astillero D.J.C.; Cruz, M.S.D.: Development of Microcontroller-Based Biometric Locker System with Short Message Service. Lecture Notes on Software Engineering, Vol. 4, No. 2. Pp. 103-106, 2016.
[3] Annie, O.P.; Rahul A.P.; Prenav V.; Ponni, S.; Renjith, N.: Design and Implementation of a Digital Code Lock. International Journal of Advanced Research in Electrical Electronics Instrument Engineering. Vol 3, Issue 7, pp. 604-607, 2014.
[4] Amuda, F.A.; Tennyson, D.I.: Design and Implementation of a Fingerprint Lock System, IOSR Journal of Engineering (IOSRJEN), Vol. 7, pp. 13-19, 2017.
[5] Patil, B.S.; Mahajan V.A,; Suryawanshi S.A.; Pawar, M.B.: Automatic Door Lock System Using Pin on Android Phone, International Research Journal of Engineering and Technology (IRJET), Volume. 05, Issue 11, pp. 1007-1011, 2018.
[6] Nayana, R.; Shashidhar R.: Smart Door Lock System, International Journal for Modern Trends in Science and Technology, Vol. 05, Issue 02, pp. 36-38, 2019.

ANNALS of Faculty Engineering Hunedoara – International Journal of Engineering
ISSN 1584 - 2665 (printed version); ISSN 2601 - 2332 (online); ISSN-L 1584 - 2665