Journal of Advances in Science and Engineering 7 (2022) 18 – 23

Journal of Advances in Science and Engineering
(JASE)

Journal homepage: www.sciengtexopen.org/index.php/jase

Design and implementation of a fingerprint-based biometric access control system

E. Esekhaigbe [a]*, E. O. Okoduwa [b]

[a, b] Department of Electrical/Electronic Engineering, Ambrose Alli University, Ekpoma, Nigeria

ARTICLE INFO

Article history:
Received 29 March 2022
Received in revised form
17 June 2022
Accepted 28 June 2022
Available online
14 July 2022

Keywords:
Arduino
Biometric access control
C-Language
Fingerprint
MATLAB
Minutiae

ABSTRACT

Security systems are often penetrated by sophisticated criminals, thus there is always a need for new solutions to be devised to give sufficient security to houses and other locations. The goal of this project is to build and deploy a fingerprint-based biometric access control system. The fingerprint is a pattern of ridges and valleys on the surface of a fingertip. Among various biometrics, fingerprint recognition is the most extensively and internationally accepted biometric because of its uniqueness, accuracy, cost-effectiveness, non-transferability, and ease of use. Presented is the system architecture for the system development that demonstrates component augmentation, detail extraction, and matching methodologies. MATLAB and the programming language C were used to develop a software application that was used to build algorithms for improvement, minutiae extraction, and matching processing. The software works by extracting meaningful features known as minutiae points from the person's fingerprint, then records and stores these minutiae points to verify the person's identity in the future. The resulting minutiae information is used to find matching fingerprints and to register these fingerprints in the system database. Finally, a verification system and identification system were realized. The proposed automatic door access control system was implemented using the Arduino Atmega 328p microcontroller. The proposed system was tried-out in real-time, and its performance was deemed adequate.

1. Introduction

The primary concern of people is security. Thus, it befits us to proffer workable remedies and ideas to protect our possessions and privacy. Home security and possessions may be a serious concern for individuals, businesses, or governments. Property security and intrusion into properties have been a critical concern since the start of civilization [1]. Door security controls may now easily safeguard a facility. Unauthorized individuals are denied entry and their movements are tracked [2]. One of the ways to regulate entrance to certain areas is via locking indoors [3]. As technology evolves and the world around us becomes more digital, protecting sensitive information becomes more difficult. Passwords and keys were formerly regarded to be sufficient for secure data transfers, and other reasons. However, sophisticated hacker attacks and unauthorized internet users have exposed them [4]. With the advancement in technology, culminating in the emergence of different sophisticated devices available for use on the internet, the need to secure data from hackers and unauthorized individuals becomes increasingly apparent. Passwords may assist in avoiding this. The problem is that users may reuse passwords across many devices. Furthermore, these passwords might be exchanged and broken by someone with advanced technical abilities. Locksmiths developed security technologies and equipment throughout the development and fall of civilizations [5].

According to [6], fingerprint biometrics is considered to be the most trustworthy and universally acceptable biometric recognition; because of its traits of uniqueness, accuracy, non-transferable, ease of use and cost-effectiveness. Trauring [7] published the first scientific paper on biometric recognition based on fingerprint matching, the study aimed to provide a method of decentralized automatic identity verification using minutiae in finger-ridge patterns. Subsequently, biometric recognitions based on other traits (face, voice, iris, signature and hand geometry) were developed. Thus, it is over 58 years that the first

* Corresponding author
E-mail address: emmaesekhaigbe@yahoo.com
https://doi.org/10.37121/jase.v7i1.183

research publication on biometric recognition was produced [8-10]. Wayman [11] concluded that a brief assessment of biometric history indicates that much of what is considered to be "new" in biometrics was genuinely envisaged decades ago. There's still work to be done, but it's better to focus on what's new than to recycle old studies. Jain et al. [12], reviewed the state-of-the-art biometric identification and identified major challenges. Moreover, their findings highlighted the great potential for basic and applied biometric research. As a result, scientists and engineers were inspired to explore biometrics, leading to greater interest in developing biometric solutions for resource-constrained devices.

To address the drawbacks and disadvantages of traditional locks, smart security solutions that are easy to use, accessible, and trustworthy have been developed; aside from the use of smartcards and biometrics [13,14]. Advancement in technology spurs people to look out for sophisticated security gadgets which are flexibly beneficial for home use. Thus, researchers are attempting to build intelligent and user-friendly security devices for smart homes in response to the growing demand. Based on their intended use, devices are created from a variety of perspectives. Some security systems are concerned with unlawful entry into the house [15-17]. Some have to do with safety from fire consequent upon gas leakage [18], and others covered the use of a password or biometric lock for access to the home [19-21].

2. Methodology

System components include the following units: power supply, fingerprint module, LCD, H-bridge motor, microcontroller, as well as control buttons, buzzer and signal LEDs. The supply unit powers the microcontroller, the fingerprint module and the LCD with a controlled 5V. Additionally, it provides the same voltage to the motor unit. The microcontroller unit acts as the system’s nerve centre, directing the operations of the other elements. When a fingerprint picture is identified by the fingerprint module, it is routed via the system’s database where it is compared with previously recorded image scans. Upon recognition, the micro-controller permits the H-bridge motor to regulate the automated sliding door opening. The functional block diagram of the proposed system is shown in Fig. 1.

2.1. The Power Supply Unit

A 220/12V step-down transformer powers the system. The secondary side of the transformer's output was rectified using a diode bridge rectifier. Filter capacitors in the circuit (Fig. 2) assist filter residual AC (ripples). The system needed a controlled 5V DC to power the various components, hence the LM7805 was chosen. The voltage regulator transforms rectified 12V to 5V. Due to the high frequency and high current pulse loads of the system, ceramic capacitors were used in the power supply design.

2.2. Fingerprint Module Unit

The fingerprint module unit stores pre-scanned fingerprints. It is retrieved at the time a user inserts his finger on the module unit. The module's behaviour and pattern were analysed from its datasheet. To enable the module, the power source must offer 5V. The pins of the module output respectively link pins 2 and 3 of the Atmega328p. Fig. 3 shows the fingerprint module.

2.3. Microcontroller Unit

An 8-bit Atmega328p microcontroller, shown in Fig. 4, is used in this study. The microcontroller uses Vcc, GND, TX, RX (the serial port) to operate the H-bridge switch. It consists of a memory that can only be read (ROM). Ports B, C, and D were employed for diverse reasons. In this study, the timer interrupt service approach and ADC function were employed. The signal LEDs on the microcontroller were programmed using PD4-PD7, while the modules were set up using PD0 and PD1, the respective module's transmitter and receiver. PC1, PC2, PC3, and PC4 were the trigger pins for the H-bridge motor, and PB0 through PB5 were the LCD pins. Pin UT1 of the ADC keypad was connected to PC0 through down resistors, and the CPU was linked to the emergency and setting buttons.

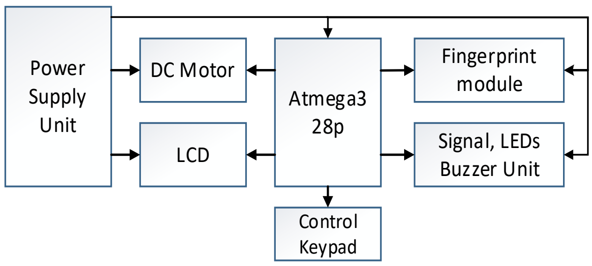

Fig. 1 Functional block diagram of the proposed system.

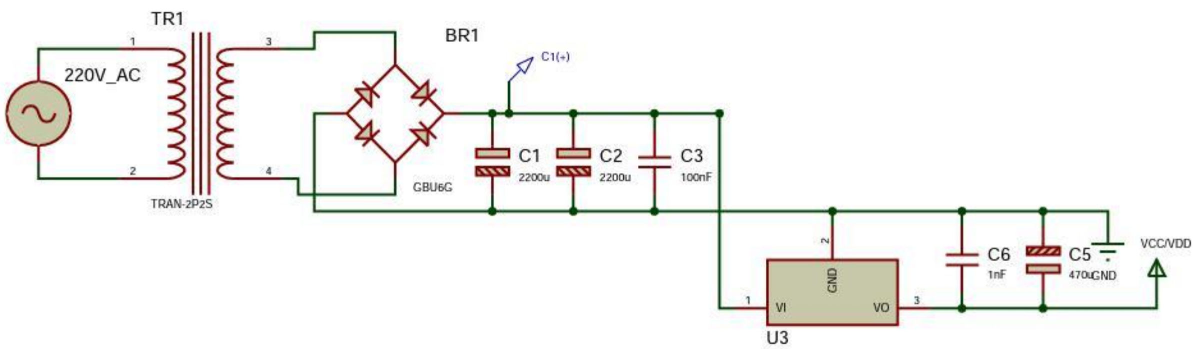

Fig. 2 Power supply unit.

Fig. 3 Fingerprint module unit.

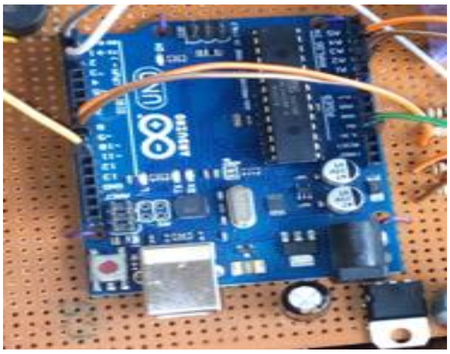

Fig. 4 The microcontroller unit.

When the emergency button is hit, the micro-controller opens the automated door whenever a fingerprint is scanned, regardless of whether or not the fingerprints are authorized. The settings button grants the chosen officer access to user control or admin mode. The user may alter the administrator's fingerprint and add or delete fingerprints from the system's database. PC4 encodes the escape button into the microcontroller so that the door may be opened from the inside. To satisfy system requirements and avoid component damage, resistors were employed to lessen the sensitivity to fluctuations in Vcc voltage. Connecting the reset, enter, exit, and emergency buttons to Vcc will restart the system.

2.4. The Motor H-Bridge Driver Unit

This unit controls the sliding door's motion using H-bridge switches and an electric motor. The supply unit furnishes the motor (a DC motor that may be operated in either direction) with 5V. The microcontroller controls this machine by simply switching the power polarity and applying a low-level logic input signal. The microprocessor changes the polarity of the motor to regulate its direction. To move the motor forward, switch TR1 and TR4 must be activated. Logic 1 activates BC557 to convey a voltage signal into M1 while logic 0 triggers TR4. The 1N4004 grounds M2, leading the motor to be driven forward by the H-Bridge as depicted. To reverse the direction of the motor switches TR3 and TR2 are closed. The microcontroller applies logic 1 to TR3 and logic 0 to TR2 to complete the circuit and move the motor in the opposite direction. The resistors were added to modify the system's sensitivity.

2.5. LCD Unit

The supply unit provides 5V to the liquid crystal display. It shows pre-programmed instructions and data from the system CPU to the user to improve the system's user interface. The LCD pins are linked to microcontroller port B. The power LED "D1" is powered by the power supply and shows that the system is turned on. D5" LED signifies that the system is in "normal mode," while the "D2" LED indicates that a user has been authorized to gain access. The two LEDs are controlled by the main CPU.

2.6. The Flow Chart Analysis

Regarding the flowchart diagram in Fig. 5, when the system is turned "ON," it takes 5 seconds to configure all hardware, including the control buttons, fingerprint module, and microcontroller, while the LCDs indicate the system's status. It determines if the administrator button has been touched and asks the user to input control buttons. If no card is inserted, the regular mode is entered. If an administrator has not yet been established, the device scans your fingerprint to generate one and thereafter asks the user to push the reset button. If there is already an administrator, the admin menu is accessed by scanning for the administrator's fingerprint, if accessible. If not accessible, "fingerprint not found" is shown. Using the control buttons, the admin menu provides choices to (1) add the user, (2) delete the user, (3) change admin, (4) empty the database, and (5) leave the menu.

The door opens, shuts, and decrements the count if the button is pressed from the inside when the door is initialised during normal mode operation. From the outside, where the fingerprint sensor is located, the LCDs the instruction "To enter, put your finger on the fingerprint scanner”. If a person is favourably scrutinised, access is granted while the count is incremented before shutting straightaway. On the condition that it is not in agreement with any in the database, the person is prompted to retry.

3. Results and Discussion

Shown in Table 1 are designed values and selected values of the components that were used in the study. The components were connected and soldered. Thereafter, the design circuit was tested and found to work as shown in Figs. 6 and 7 while the front view of the designed system is shown in Fig. 8.

3.1. System Performance

Following the successful implementation of the design, its performance was tested. This was done to validate the operating performance of the system developed. The results are depicted in Table 2.

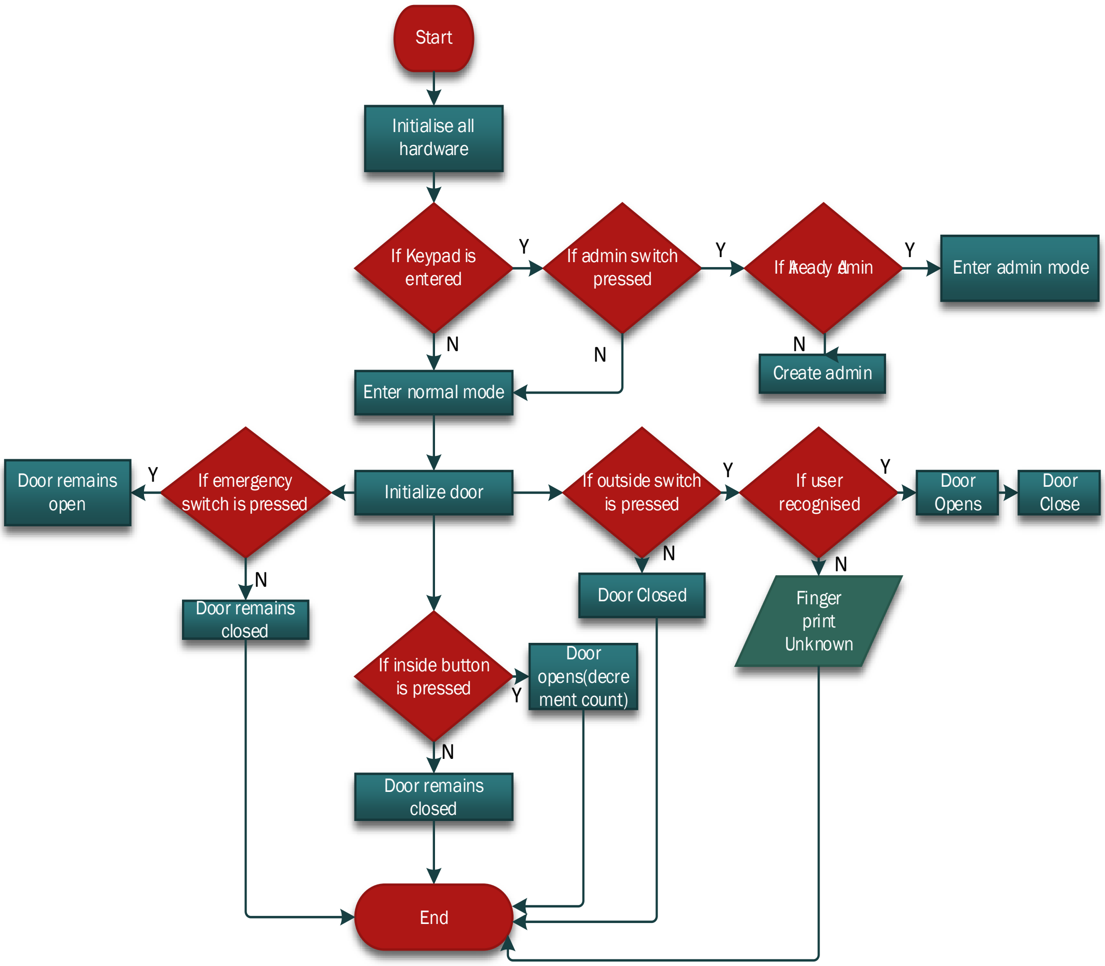

Fig. 5 The flow chart of proposed system functionality.

Table 1: Parameters of the Designed System

Components	Designed Values	Selected Values
R1	33.94Ω	34Ω
R2	4kΩ	4kΩ
R3	9.8kΩ	10kΩ
R4	10.3kΩ	10kΩ
R5	3.2kΩ	3kΩ
R6	1.1kΩ	1kΩ
C1	1000.05µF	1000µF
C2	2200µF	2000µF
C3	2200µF	2000µF
C4	2200µF	2000µF
C5	470µF	470µF
C6	1nF	1nF

Fig. 7 Components mounted in casing.

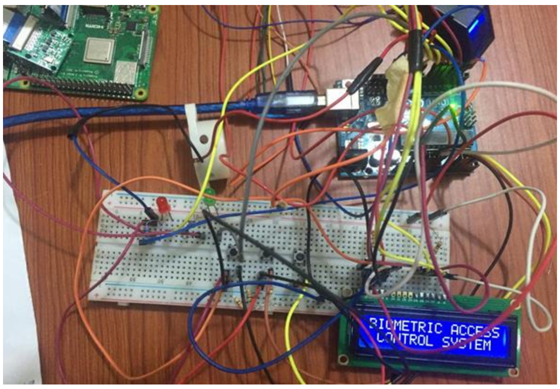

Fig. 6 A prototype of system design on a breadboard.

Fig. 8 Front view of the designed system.

Table 2. System performance.

Parameters	Theoretical Values	Measured Values	Variation (%)
AC Mains (V_{ac})	220V	200V	9.1
Transformer Output	12V	11.3V	5.8
Rectifier Output	12V	11.5V	4.2
Voltage Regulator	5V	5V	0
Scanning Rate	2	2	0

It was observed that:

(a) Access to the restricted area was only granted to persons whose fingerprint minutiae have been extracted, recorded and stored.

(b) When access is granted, the door remains opened for 4secs and thereafter closes; to prevent unauthorised users.

(c) Alarm is activated if an unauthorised user is attempting to forcefully gain access.

3.2. Discussion

The measured voltage of the power supply unit was 5.45V and it was approximately equivalent to the voltage needed for the components to operate. The fingerprint module successfully fulfilled its function of identification and comparison. As a result, it was observed that the motor unit turned in either direction as directed by the microcontroller unit and the H-bridge circuit. During system setup, the LCD played the role of verification concerning program code as well as the exact individuals gaining access. When the system was powered on, the liquid crystal display was confirmed to operate correctly. Programming and circuit connections were implemented on the microcontroller. In addition, the microcontroller's C language program code was error-free, as the LCD, H bridge motor unit, and fingerprint module all performed as planned. Using a voltage divider under typical operating circumstances, the voltages flowing through the control buttons were 0V, 2.5V, and 4V. Normal operation of the buzzer was seen when an unidentified user fingerprint image was discovered.

4. Conclusion

Within the scope of this research, both the conception and execution of an automated fingerprint door entry system were described. The Arduino Atmega 328p microcontroller was used in the construction of the automated door access control system that was presented. The performance of the developed system was evaluated in the context of real-time environments, and it was determined to be adequate. It is feasible that the inclusion of security features, such as fingerprint and password systems, will distinguish and make the system more competitive in the marketplace. Numerous other security technologies may be implemented into the system to enhance its security since the future scope of this work is highly expansive. As an example, consider an iris scanner for visual identification. Additionally, the system may be strengthened by employing machine intelligence methods to expedite as well as simplify the identification of individuals utilizing facial recognition technology and a database of well-known thieves. The scope of this effort in the future is exceedingly expansive.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

ORCID

E. Esekhaigbe https://orcid.org/0000-0002-5082-4169
E. O. Okoduwa https://orcid.org/0000-0001-5899-4720

References

[1] S. Emakpor, E. Esekhaigbe, “Development of an RFID-based security door system,” *J. Elect. Control Technol. Res.*, vol. 1, pp. 9 - 16, 2020.

[2] W. O. Winda, S. Mohammed, “Intelligent voice-based door access control system using adaptive-network-based fuzzy inference systems for building security,” *J. Comp. Sci*., vol. 3, pp. 274-280, 2007.

[3] B. O. Omijeh, G. O. Ajabuego, “Design analysis of a security lock system using pass-code and smart-card,” *IOSR J. Elect. Comm. Eng*., vol. 4, pp. 64-72, 2013.

[4] M. S. Okundamiya, S. Emakpor, “Design and control strategy of a security door system using radio frequency signal,” *2017 IEEE 3rd Int. Conference on Electro-Technology for National Development*, pp. 406-412, 2017.

[5] W. Dongdong, “Introduction of capacitive fingerprint sensor packaging technology," *2017 18th Int. Conference on Electronic Packaging Technology*, pp. 130-134, 2017.

[6] J. B. Awotunde, O. W. Fatai, M. B. Akanbi, D. I. Abulkadir, O. F. Idepefo “A hybrid fingerprint identification system for immigration control using the minutiae and correlation methods,” *J. Comput. Sci. Appl*., vol. 22, no. 1, pp. 15-23, 2015.

[7] M. Trauring, “Automatic comparison of finger ridge patterns,” *Nature*, vol. 197, pp. 938-940, 1963.

[8] J. G. Daugman, “High confidence visual recognition of persons by a test of statistical independence,” *IEEE Trans. Pattern Anal. Mach. Intell*., vol. 15, no. 11, pp. 1148-1160, 1993.

[9] W. W. Bledsoe, “Man-machine facial recognition,” Technical Report, PRI 22, Panoramic Research Inc. 1966

[10] A. J. Mauccri, “Feasibility study of personal identification by signature verification,” Technical Report SID 65, Defence Technical Information Centre, North America Aviation, 1965.

[11] J. L. Wayman, “The scientific development of biometrics over the last 40 years,” K. De Leeuw, J. Bergstra, (eds.), In: *The History of Information Security*, Elsevier Science B.V., pp. 263-274, 2007.

[12] A. K. Jain, K. Nandakumar, A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognition Letters*, vol. 79, pp. 80-105, 2016.

[13] S. Palka, H. Wechsler, B. A. Hamilton, "Fingerprint readers: Vulnerabilities to front- and back- end attacks," *2007 First IEEE Int. Conference on Biometrics: Theory, Applications, and Systems*, pp. 1-5, 2007.

[14] C. Lin, A. Kumar, "Matching contactless and contact-based conventional fingerprint images for biometrics identification," *IEEE Trans. Image Process*., vol. 27, no. 4, pp. 2008-2021, 2018.

[15] J. Bangali, A. Shaligram, "Design and implementation of security systems for smart home based on GSM technology", *Int. J. Smart Home*, vol. 7, no. 6, pp. 201-208, 2013.

[16] R. Hasan, M. M. Khan, A. Asehek, I. J. Rumpa, "Microcontroller based home security system with gsm technology," *Open J. Safety Sci. Technol*., vol. 5, pp. 55-62, 2015.

[17] M. Potnis, A. Chimnani, V. Chawla, A. Hatekar, "Home security system using gsm modem," *J. Eng. Res. Appl*., vol. 5, no. 4, pp. 143-147, 2015.

[18] L. Fraiwan, K. Lweesy, A. Bani-Salma, N. Mani, "A wireless home safety gas leakage detection system," *2011 1st Middle East Conference on Biomedical Engineering*, pp. 11-14, 2011.

[19] A. Aditya Shankar, P. R. K. Sastry, A. L. Vishnu Ram, A. Vamsidhar, "Finger print based door locking system," *Int. J. Eng. Comput. Sci*., vol. 4, no. 3, pp. 10810-10814, 2015.

[20] K. W. Nafi, T. S. Kar, S. A. Hoque, "An advanced door lock security system using palmtop recognition system," *Int. J. Comput. Appl*., vol. 56, pp. 18-26, 2012.

[21] A. Kawale, "Fingerprint based locking system," *Int. J. Sci. Eng. Res*., vol. 4, no. 5, pp. 899-900, 2013.