Fingerprint Based Door Lock System

A.T.M. Mustafa Masud Chowdhury

Department of Computer Science and Engineering, Southern University of Bangladesh.

Article Info

Article history:

Received : April 23, 2023
Revised : May 14 , 2023
Accepted : May 20, 2023

Keywords:

Biometrics
Fingerprint
RFID
Alarm
Security
Authentication

ABSTRACT

Security measures have assumed a pivotal role in various settings such as offices, institutions, libraries, and laboratories. Their purpose is to safeguard confidential data from unauthorized access by third parties. In contemporary times, it is imperative to have security systems in place at all times to safeguard valuable data and financial assets. The present study introduces a door opening system that utilizes fingerprint recognition technology to enhance security measures. This system has potential applications in a variety of settings, including financial institutions, educational institutions, and other organizations. Various authentication methods such as password and RFID exist, however, this particular method is deemed to be the most efficient and dependable. This project is utilizing two distinct technologies, namely embedded systems and biometrics, in order to enhance the security of bank lockers and streamline operational processes. The prevention of unauthorized access is achieved through the implementation of a locking mechanism that securely stores the biometric data of one or more authorized individuals. The process of authentication involves the sensing of a fingerprint by a sensor, which is subsequently validated. In the event of a successful fingerprint match, the door will be unlocked through an automated process. Conversely, if the fingerprint does not match, an audio amplifier will activate a buzzer to alert individuals in the vicinity.

Corresponding Author:

A.T.M. Mustafa Masud Chowdhury
Department of Computer Science and Engineering
Southern University of Bangladesh.
Email: mustafamasudcse@gmail.com

1. INTRODUCTION

In today's fast-paced and competitive environment, ensuring security of confidential possessions is a paramount concern. It is increasingly challenging for individuals to manually devise effective measures to safeguard their belongings. Alternatively, the individual discovers an option that can offer comprehensive security while also being automated. In the contemporary networked society, individuals have the convenience of accessing their personal information at any time and from any location. However, this convenience also exposes them to the potential risk of unauthorized access by others who can also access the same information with ease. Due to the potential hazards involved, there has been a growing interest in personal identification technology that is capable of distinguishing between authorized users and fraudulent individuals [1]. Commonly employed methods for authentication include passwords, identification cards, and

PIN verification [2, 3]. However, these methods are not without their drawbacks, as passwords are vulnerable to hacking and cards may be susceptible to theft or loss. Fingerprint recognition is considered the most secure system due to the unique nature of each individual's fingerprint, which ensures that no two fingerprints are identical. The field of biometrics frequently encompasses research on various methods of identification and authentication, such as fingerprint, facial, iris, vocal, signature, and hand geometry recognition and verification. Several alternative modalities are currently undergoing different phases of development and evaluation. Fingerprint biometric trait is considered to be one of the most optimal traits due to its favorable mismatch ratio, high accuracy in terms of security, and reliability.

2. BACKGROUND

Numerous endeavors have been undertaken to ensure the safety and security of all residences. Currently, a comprehensive and up-to-date security solution has yet to be developed.

a) Lock and Key System

The initial measure taken towards ensuring security involved the implementation of the lock and key mechanism. The security protocol implemented in this system adhered to the principle of "one key for one lock". At the outset, this system was deemed to offer the highest level of security. However, this assertion was subsequently refuted by the observation that a single lock can be readily duplicated to produce multiple keys. Therefore, it can be inferred that the aforementioned system is antiquated and lacks adequate security measures [4].

b) Password Authentication

The subsequent tier of security employs a password as a means of authentication. This system stores the passwords of authenticated users for the purpose of validation. The utilization of password authentication within a system offers a significant level of security to its users, as it functions as a confidential mechanism for authorized individuals. This system is susceptible to the drawback whereby unauthorized individuals can obtain passwords through a brute force attack, which involves systematically attempting all possible combinations. This is also one of the hundreds of attempts made to provide security [5].

c) Authentication by RFID card

The subsequent stage in the progression of technological advancements aimed at ensuring security involved the utilization of RFID card authentication. The implementation of this system resulted in an improvement in the overall security measures. Admittance is exclusively permitted to the individual whose RFID code corresponds with the sanctioned code. This system exhibits the drawback of RFID card duplication, thereby enabling any individual in possession of said card to gain access to the door [6].

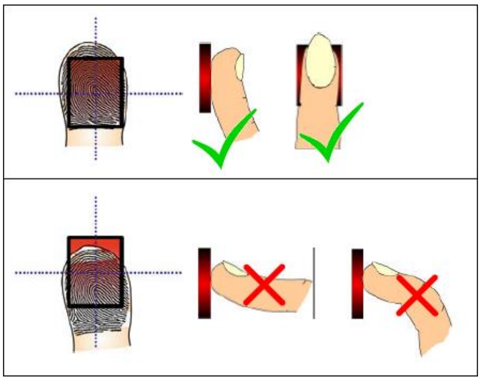


Figure 1. Correct way to access Fingerprint sensor [6]

3. METHODOLOGY

The system is constructed based on two fundamental constituents, namely hardware and software. In this context, we aim to explore the hardware components of our system and employ a block diagram and flow chart to gain insight into the system's functionality through the integration of software and hardware.

a) Hardware Specification

The hardware components utilized in this study include a Crystal oscillator, Capacitor, Resistor, Diode, Fingerprint Recognition module, SD card for the storage of fingerprint data, relay, voltage regulator, and LCD Display.

Crystal oscillators employ the resonance of a piezoelectric crystal, usually quartz, to produce an accurate electrical signal. They are widely employed in timekeeping, digital circuits, and radio equipment for frequency stabilization. Quartz crystals are a frequently utilized component, with an annual production of billions of units to cater to diverse consumer devices [7]. A capacitor stores electrical energy in an electric field between conductors separated by an insulator. The application of a voltage results in the accumulation of electric charge on the conductive materials. It has capacitance measured in farads. Capacitors are utilized in electrical circuits and exhibit diverse configurations and dielectric materials [8]. A resistor is an electronic element that restricts the flow of current and diminishes voltage levels within circuits. In electronic circuits, signal levels are adjusted, power is controlled, and diverse functions are performed through its utilization. Resistors are classified into two types, namely fixed and variable resistors, and exhibit a broad spectrum of resistive values. They are widely used in electrical networks and electronic devices [9]. A diode is a binary electronic component featuring two terminals that permits the flow of electrical current in a singular direction, while impeding its flow in the opposite direction. The material composition of the device can either be semiconductor or vacuum tube. Diodes were first discovered in 1874 and are commonly made of silicon today [10]. The LCD technology is a type of flat panel display that employs liquid crystals to regulate the transmission of light. It finds application in diverse domains such as computer displays, television sets, timepieces, and mobile devices. LCDs offer energy efficiency, and a wide range of screen sizes, and do not suffer from image burn-in. According to reference [11], cathode ray tube (CRT) displays were replaced by a new technology that gained worldwide popularity. A voltage regulator is a device that ensures a consistent voltage level through the utilization of either electromechanical or electronic components. The device in question serves to stabilize both AC and DC voltages and finds utility in a diverse range of applications, including but not limited to computer power supplies, alternators, and power distribution systems, with the primary aim of guaranteeing a consistent voltage output [12]. The FPM10A module is utilized for biometric authentication through fingerprint recognition. The system enables users to complete the registration and authentication of their fingerprints. The module is capable of acquiring and evaluating fingerprint data, thereby furnishing a dependable and secure technique for identification and access control across a range of applications, including but not limited to security systems and personal devices [13, 14, 15].

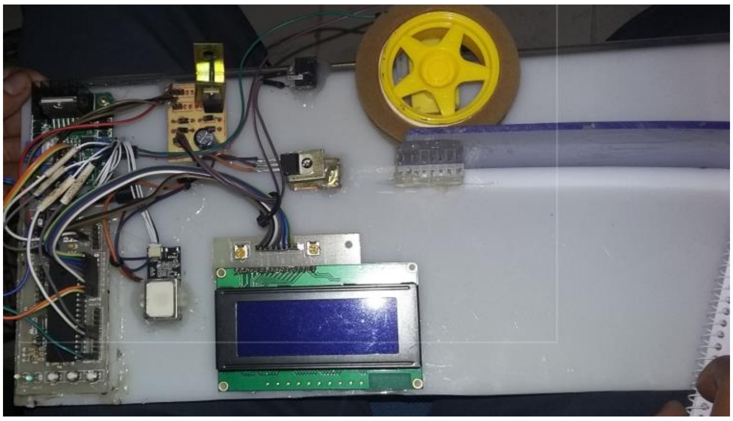


Figure 2. Proposed Developed Module

b) Block Diagram and Flow chart of the model

Software utilization is feasible in this context. The Mikro PRO for PIC is a highly potent development instrument designed for utilization with PIC microcontrollers. The integration of PIC microcontrollers and C programming language provides an effective approach to developing embedded systems. The package comprises a sophisticated Integrated Development Environment (IDE), a compiler that conforms to the American National Standards Institute (ANSI) standards, libraries for hardware, documentation, and pre-existing executable instances.

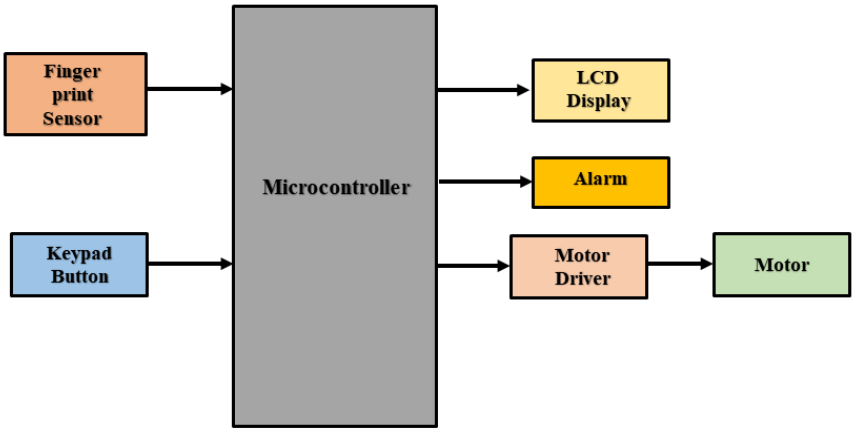


Figure 3. Block diagram of the system we proposed

The block diagram illustrates that the microcontroller receives data from both the fingerprint sensor and keypad. It then processes this data and displays the output on the screen while also providing instructions to the motor driver.

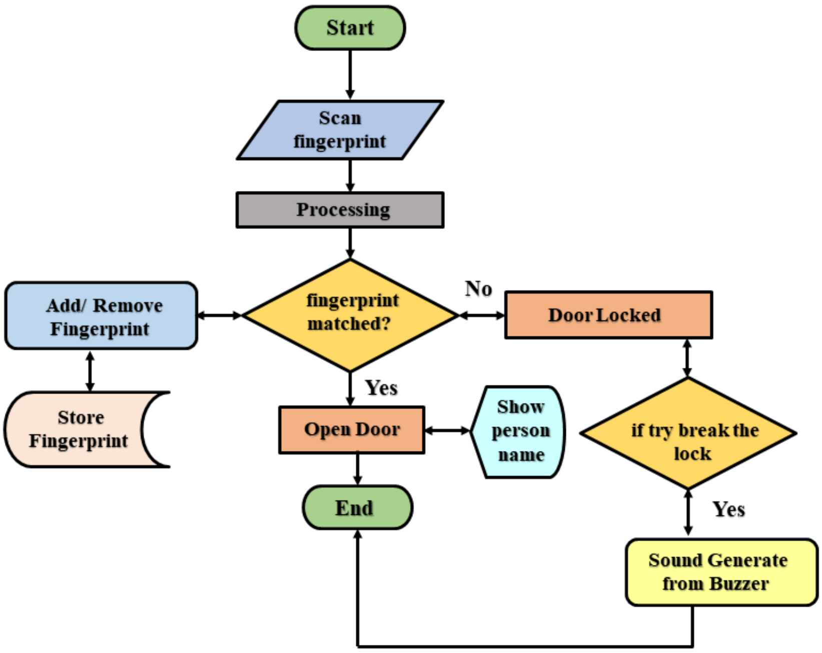


Figure 4. FlowChart of the system we proposed

We can see in the flow chart that our system is working in 4 steps

1) Add Finger

During the addition process, it is necessary to input a minimum of five images of fingerprints. Subsequently, personal information and photographs of the individuals whose fingerprints were added to the program must be included for the purpose of future identification and enumeration [13, 14, 15].

2) Identity finger

Upon pressing a finger onto the fingerprint screen, the system initiates an automatic verification process to compare the captured fingerprint image with the pre-registered fingerprints. If a match is detected, the door will unlock automatically. Following this, the door will automatically close after a predetermined duration, as programmed, and the room light switch will be activated. The system will capture and store the data pertaining to the individual entered [13,14,15].

3) Delete Finger

In this process, we can delete old fingerprints and also add new fingerprints.

4) Locked system

In the event that an individual endeavors to gain entry to a restricted area by persistently endeavoring to unlock the door with an unauthenticated fingerprint, the system will initiate a master lock mechanism and prompt an audible security alert.

4. RESULTS AND DISCUSSION

We have highlighted below that our developed system has been tested in several steps

Step 1: When power is supplied to the board, the initial displays on the LCD are as shown below.

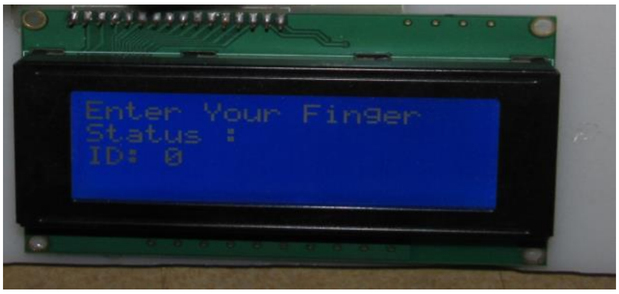


Figure 5. Finger print test step 1

Step 2: Scanning the finger.

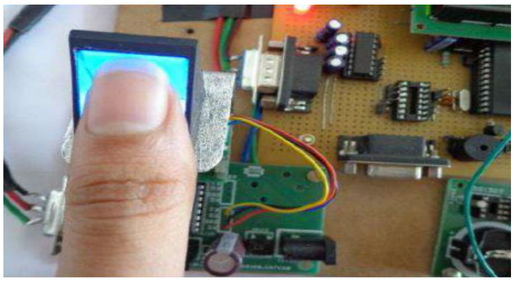
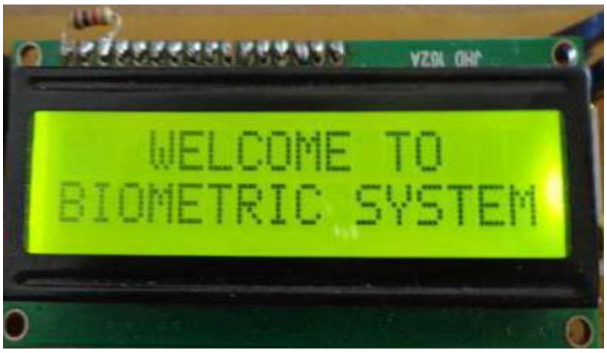


Figure 6. Finger print test step 2

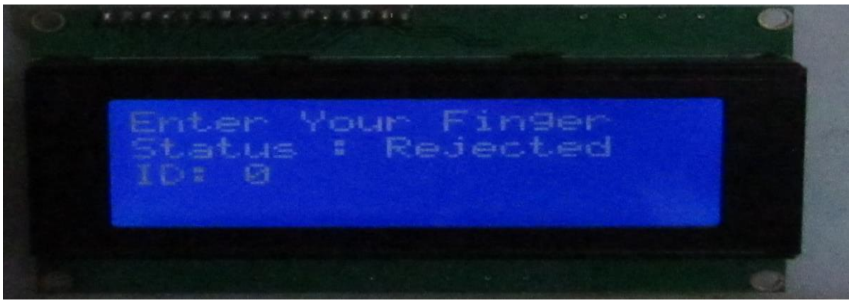
Step 3: When the persons fingerprint matches, display on LCD.



WELCOME TO
BIOMETRIC SYSTEM

Figure 7. Finger print test step 3

Step 4: After work has been completed, the door will be open.



Enter Your Finger
Status : Rejected
ID: 0

Figure 8. Finger print test 4

Step 5: After few minutes the door is automatically closed again.

Step 6: When entered finger is incorrect the LCD show like below:

Table 1. Result Analysis

Entering Finger	Display Status	Buzzer Working	Detection Time	Door Opening	Door Closing
Added finger	Accepted	off	1 sec	yes	yes
Added finger	Accepted	off	1 sec	yes	yes
Wrong finger	Rejected	On	3 sec	no	no
Wrong finger	Rejected	On	3 sec	no	no
Wrong finger	Rejected	On	3 sec	no	no
Wrong finger	Rejected	On	1 sec	no	no

5. CONCLUSION

In order to conduct a comparison between saved and scanned images, a microcontroller operating in user mode is interfaced with a fingerprint module. In order to gain access to lockers, individuals who have been granted permission possess specific fingerprint images that are linked to their identification. The 8051 microprocessor manages to scan, and the locker is unlocked by entering a password on the keypad. The door can be closed by pressing a key on the keypad. The system alerts the user of unauthorized scans or incorrect passwords through an audible alarm. The present user has the ability to enroll a new fingerprint and delete the fingerprint data of the previous user. It is feasible to modify passwords. The system has been designed with a focus on ensuring transaction security, locker security, and passport verification through the utilization of a fingerprint scanner. Biometric authentication offers reliable security and surpasses existing technologies.

REFERENCES

[1] Mukesh Kumar Thakur, Ravi Shankar Kumar, Mohit Kumar, Raju Kumar “Wireless Fingerprint Based Security System using Zigbee” , International Journal of Inventive Engineering and Sciences (IJIES) ISSN: 2319–9598, Volume-1, Issue-5, April 2013.

[2] Mahendra, Apoorva, Shyam, Pavan, and H. Bedi, “Fingerprint image identification system: An asset for security of Bank Lockers,” *Digital Forensics and Internet of Things*, Vol. 10, Issue. 6, 2022, Doi:10.1002/9781119769057.ch13

[3] M. Jain and A. Khurana, “Overview of biometric fingerprint identification,” *International Journal of Trend in Scientific Research and Development*, vol. Volume-2, no. Issue-3, pp. 2721–2725, 2018. Doi: 10.31142/ijtsrd14101

[4] R. M. Lourde and D. Khosla, “Fingerprint identification in biometric SecuritySystems,” *International Journal of Computer and Electrical Engineering*, Vol. 2, Issue. 3, pp. 852–855, 2010. doi:10.7763/ijcee.2010.v2.239

[5] A. K. Jain, Jianjiang Feng, A. Nagar and K. Nandakumar, "On matching latent fingerprints," 2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, Anchorage, AK, USA, 2008, pp. 1-8, doi: 10.1109/CVPRW.2008.4563117.

[6] P. V. Reddy, A. Kumar, S. M. Rahman, and T. S. Mundra, “A new antispoofing approach for biometric devices,” *IEEE Transactions on Biomedical Circuits and Systems*, vol. 2, no. 4, pp. 328–337, 2008. doi:10.1109/tbcas.2008.2003432

[7] “Reported Crystal oscillator vs Resonator,” Circuit Digest - Electronics Engineering News, Latest Products, [online] Articles and Projects, Available online https://circuitdigest.com/article/crystal-oscillator-vs-resonator [accessed April 15, 2023].

[8] Mary Lourde R and Dushyant Khosla, “Fingerprint Identification in Biometric Security Systems”, International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010

[9] “Reported Resistor, Available online” Wikipedia, https://en.wikipedia.org/wiki/Resistor [accessed April 10, 2023].

[10] “Reported the constituents of semiconductor components - Vishay Intertechnology, Available online https://www.vishay.com/docs/84058/84058.pdf [accessed April 12, 2023].

[11] “Reported Fujitsu Technical Support Pages from Fujitsu EMEA,” Fujitsu Technical Support pages from Fujitsu EMEA, Available online https://support.ts.fujitsu.com/ [accessed April 14, 2023].

[12] J. Baidya, T. Saha, R. Moyashir and R. Palit, "Design and implementation of a fingerprint based lock system for shared access," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2017, pp. 1-6, doi: 10.1109/CCWC.2017.7868448.

[13] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, “Security and accuracy of fingerprint-based biometrics: A Review,” *Symmetry*, vol. 11, no. 2, p. 141, 2019. Doi: 10.3390/sym11020141

[14] U. Gawande, Y. Golhar, and K. Hajari, “Biometric-based security system: Issues and challenges,” *Intelligent Techniques in Signal Processing for Multimedia Security*, pp. 151–176, 2016. Doi: 10.1007/978-3-319-44790-2_8

[15] S. A. Zabidi and M.-J. E. Salami, “Design and development of intelligent fingerprint-based security system,” *Lecture Notes in Computer Science*, pp. 312–318, 2004. Doi: 10.1007/978-3-540-30133-2_40

BIOGRAPHIES OF AUTHORS

A.T.M. Mustafa Masud Chowdhury is a BSc student in the Department of Computer Science and Engineering at the Southern University of Bangladesh. He is an early-stage researcher working since 2020, an active member of the programming problem solve and computer club besides research and guiding B.Sc final year students of his department for comparative research. His areas of interest are Artificial Intelligence, Machine Learning, and IoT Solutions. With a background in system analysis and engineering design. A.T.M. has constructed a solid paradigm to meet the need for an AI-driven society. His contact email address: **mustafamasudcse@gmail.com**