Fingerprint Door Lock using Arduino UNO R3

Siddhartha Bhowmick[1], Aman Kumar[2], Sai Manas[3]

[1, 2, 3]Department of Mechanical Engineering, Dr. B. C. Roy Engineering College, Durgapur, West Bengal - 713206, India.

Abstract:
Fingerprint door locks have gained significant popularity due to their convenience and enhanced security compared to traditional lock systems. However, recent advancements in biometric hacking techniques and emerging technologies call for a more robust and reliable approach to fingerprint-based access control. This project aims to explore and implement a robust approach to enhance the security of fingerprint door locks. The study will investigate the integration of additional biometric modality along with the algorithm of advanced encryption to improve the overall security and authentication accuracy of fingerprint door lock systems.

Keywords: Fingerprint recognition, Microcontrollers, IOT, Multimodal authentication

1. Introduction

Fingerprint door lock systems have become increasingly popular due to their convenience and enhanced security compared to traditional lock mechanisms. However, researchers and security experts have identified vulnerabilities and limitations in existing fingerprint-based access control systems, highlighting the need for further advancements. This literature review aims to explore existing research on fingerprint door lock systems, biometric vulnerabilities, and multimodal authentication techniques to provide a comprehensive understanding of the subject and identify potential areas for improvement.

Research on fingerprint door lock systems has primarily focused on enhancing the accuracy, speed, and reliability of fingerprint recognition algorithms. Various fingerprint matching algorithms, such as minutiae-based, ridge-based, and correlation-based methods, have been explored to improve authentication performance. Studies have also investigated the impact of different factors, such as sensor quality, image resolution, and environmental conditions, on the reliability and effectiveness of fingerprint recognition. Research has shown that fingerprint scanners can be susceptible to spoofing attacks using artificial fingerprints, gummy fingers, or latent prints. Additionally, the low-resolution sensors or poor image quality can result in false rejections or false acceptances. The impact of factors like aging, skin conditions, and damage to fingertips on the accuracy of fingerprint recognition has also been examined. Studies on integration of palm print and vein pattern recognition has investigated the integration of palm print and vein pattern recognition with fingerprint door lock systems. To address the limitations of fingerprint-based authentication, researchers have proposed multimodal authentication techniques that combine multiple biometric modalities for enhanced security [1]. Many types of smart door locks are made to lock and unlock the door/ device which have fingerprint, RFID card, pin, password or IOT for unlocking the machine using mobile/ cell phone [2]. Amongst the usual non-public identification techniques, we especially see password and identification card techniques. However, now it's very easy to crack passwords and identity cards making these strategies unreliable. Plan has been made and put in force to a customizable and tuneable fingerprint-based totally locking device [3] which is found very powerful compared to standard commercially manufactured locking systems. In the article [4], research is being done to provide maximum security for those high-level security applications. The objective of this study is to design a clever door entry gadget using a fingerprint module with a suitable layout of hardware and software technology.

The main objective of this project is to enhance the security of fingerprint door locks by employing a fingerprint biometric approach. The specific goals include:

a) Investigating the vulnerabilities and limitations of existing fingerprint door lock systems; exploring additional biometric modalities, such as palm print and vein pattern recognition, for authentication purposes.
b) Designing and implementing a prototype fingerprint door lock system.
c) Evaluating the security and accuracy of the proposed system through extensive testing and analysis; developing advanced encryption algorithms to protect the stored biometric data and enhance the overall security of the system.
d) Assessing the usability and user experience of the multimodal fingerprint door lock system through user feedback and surveys.

2. Proposed algorithm

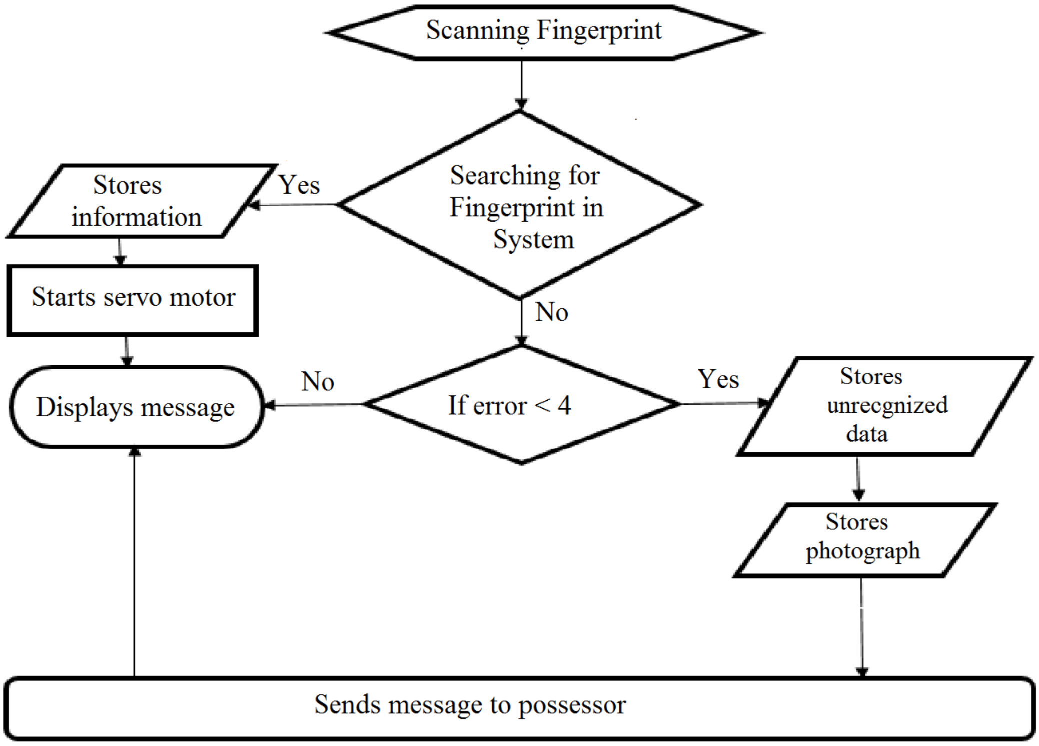

Figure 1. Flowchart of Algorithm

The fundamental idea in the back of our challenge is illustrated with the diagram above (*Figure* 1).

i. First, the finger is scanned.

ii. The scanned fingerprint, if it fits the fingerprint saved within the device, will free up the door lock by servo motor.

iii. Any person will not let to go inside if the fingerprint stored inside the gadget does not match with the scanned fingerprint. However, if the unauthorized individual tries to get entry to the door more than 3 times, then the matters will be made visible.

2.1. Initialize the system

The hardware components, including fingerprint sensor, microcontroller, and storage device are set. The system parameters, such as matching thresholds, enrolment criteria, and encryption keys are configured.

2.2. Enrollment process

To place the finger(s) the user is prompted on the fingerprint sensor. The fingerprint image is captured and the fingerprint features are extracted using a fingerprint recognition algorithm. The fingerprint template is stored securely in the storage device, associating it with the user's unique identifier.

2.3. Authentication process

Fingerprint sensor senses the placed finger of the user. The fingerprint image is captured and the fingerprint features are extracted. The stored fingerprint template associated with the user's unique identifier is retrieved. The extracted fingerprint features with the stored template is compared using a fingerprint matching algorithm. If the fingerprint authentication is successful, access is granted to the user. Otherwise, the authentication attempt is rejected.

2.4. Security measures

Advanced encryption algorithms are implemented to protect the stored biometric templates in the storage device. Communication protocols are used for security during transmission of biometric data between the sensors and the microcontroller. Additional security measures are employed, such as anti-spoofing techniques to prevent the attacks like fake fingerprints.

2.5. System evaluation

Extensive testing is conducted to evaluate the security, accuracy, and robustness of the fingerprint door lock system. The system's performance in terms of false acceptance rate (FAR) and false rejection rate (FRR) are measured.

Users' feedback is collected through surveys and post-interviews are done to assess the usability, reliability and users' experience of the system.

3. Design and Model

The sensor scans the fingerprint and converts the data into electrical pulse. Then Arduino reads it and sends the output to a power transistor, which is used to increase the voltage to operate the lock (*Figure* 2).

We used a R307 Fingerprint sensor to scan the fingerprint. A 5V wire is connected to the 5V pin of the Arduino for power supply, while a ground wire is connected to the ground pin of the Arduino for grounding purposes. The tx and rx pins of the Arduino board are connected to two additional external wires. The Arduino reads the data from the fingerprint sensor, converts it into digital signals, and sends it out through pin 12. At the end of pin 12, a power transistor is connected to amplify the voltage. The positive pin of the lock is connected to the middle pin of the amplifier, while the negative pin is connected to the GND pin of the Arduino. This configuration allows the amplified voltage to operate the lock effectively. The fingerprint sensor utilizes its scanning mechanism to capture the unique characteristics of a fingerprint. It then processes this data and converts it into an electrical pulse, which represents the fingerprint information in a digital format. (*Figure* 3).

The Arduino UNO, a microcontroller board, acts as the central processing unit in this system. It receives the electric pulse from the fingerprint sensor and proceeds to perform fingerprint verification. The Arduino UNO compares the received fingerprint data with the saved fingerprint data stored in its memory. If a match is found, indicating that the scanned fingerprint matches one of the stored fingerprints, the Arduino UNO proceeds with further actions. Upon successful fingerprint verification, the Arduino UNO generates a signal that is sent to an output pin. This signal serves as a command to activate the door lock mechanism. However, the voltage output directly from the Arduino UNO is insufficient to power the door lock effectively.

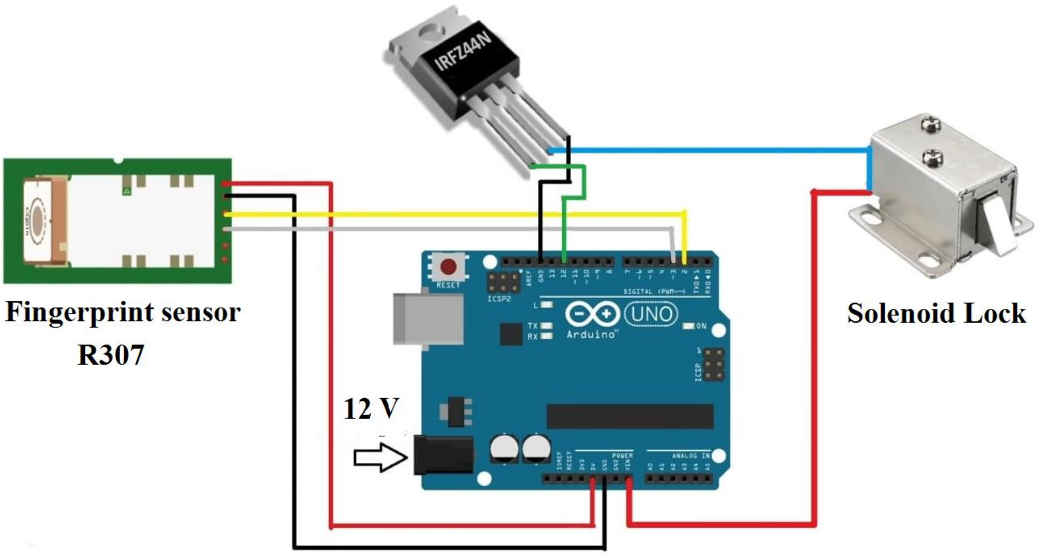

Figure 2. Schematic diagram of circuit

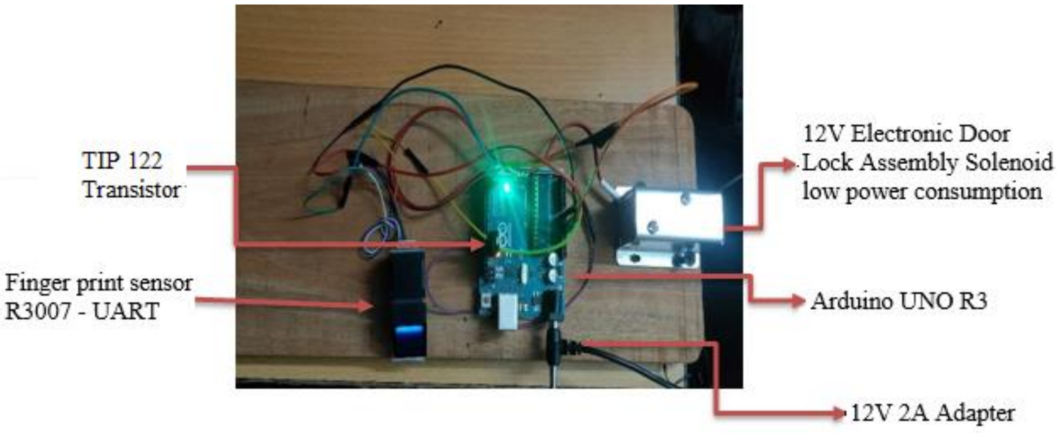

Figure 3. Working Model

4. Components used

4.1. 12V 2A DC Power supply adaptor

It is a convenient and widely used solution for providing regulated power to various electronic devices which are operated on a 12V DC power source. Before using a 12V 2A DC power supply adaptor, we have checked the polarity of the DC connector (positive and negative terminals) and matched it with the requirements of our device. Using a power supply with the wrong polarity can damage the device. Also, it is important for us that the device we are powering should not exceed 2 amps current limit; otherwise, it may cause excess power supply to overheat and subsequent damage to the system.

4.2. 20cm Male to Female jumper cable wire for Arduino

It is a type of cable commonly used in electronic projects, particularly those involving Arduino microcontrollers. It consists of a 20cm long wire with a male connector at one end and a female connector at the other end.

The male connector is designed to fit into the pins or headers on an Arduino board. These pins are typically used for input/output connections or for interfacing with various electronic components such as sensors, displays, or actuators. The male connector has exposed pins that can easily be inserted into the corresponding female headers on the Arduino-board.

4.3. 12V Electronic door lock assembly

With a solenoid and low power consumption, it is a device used for securing doors electronically. It operates at a voltage of 12 volts and is designed to consume minimal power while providing effective locking and unlocking functionality. The core component of this assembly is a solenoid, which is an electromechanical device that converts electrical energy into linear motion. The solenoid in the door lock assembly is typically responsible for actuating the locking mechanism, either by extending or retracting a bolt (latch).

4.4. Arduino UNO R3 compatible board

An Arduino UNO R3 compatible board refers to a microcontroller board that is designed to be compatible with the Arduino UNO R3. The Arduino UNO R3 is a popular development board widely used in electronics and prototyping projects.

The term "compatible" indicates that the board shares the same form factor, pin out, and functionality as the official Arduino UNO R3 board. Being not manufactured by Arduino themselves, compatible boards are designed to work with the Arduino software and libraries, allowing us to write and upload Arduino sketches to the board.

4.5. Fingerprint Sensor R307-TTL

It is a fingerprint recognition module that offers a convenient and secure way to authenticate individuals based on their fingerprints. The R307-TTL variant of the fingerprint sensor communicates using TTL (Transistor-Transistor Logic) levels. This interface allows the sensor to connect directly to microcontrollers or other TTL-compatible devices, making it easier to integrate. The R307-TTL sensor has built-in memory for storing fingerprint templates. This allows us to enroll multiple fingerprints and store them directly on the sensor module.

When using the Fingerprint Sensor R307-TTL, it's essential to follow the provided documentation and guidelines for proper wiring, initialization, and interaction with the sensor module. This will ensure optimal performance and accurate fingerprint recognition.

4.6. TIP 122 Transistor

The TIP122 transistor is a popular NPN (negative-positive-negative) power transistor that is commonly used for switching and amplification purposes in electronic circuits.It is important to consult the transistor's datasheet and application notes for specific information regarding pin configurations, voltage ratings, current limits, and other relevant details while integrating the TIP122 into the circuit design.

5. Conclusion

Fingerprint door locks provide a high level of security by utilizing unique biometric information. Each individual's fingerprint is unique, making it extremely difficult for unauthorized individuals to replicate or spoof. This significantly reduces the risk of unauthorized access, as fingerprints cannot be duplicated easily like traditional keys or access cards.

Fingerprint door lock systems provide an inherent audit trail. Each entry or access attempt is associated with a unique fingerprint, allowing for accurate tracking of who accessed the premises and when. This feature is particularly beneficial for organizations or institutions that require detailed records for security and accountability purposes.

Fingerprint door lock systems can easily be integrated into the existing security systems or standalone installations. They offer scalability, allowing for easy enrollment and removal of users as needed. Additionally, they can be deployed in various environments, such as homes, offices, or high-security facilities, providing flexibility in the application.

In conclusion, the project aimed to enhance the security of the door lock systems. The project's outcomes contribute to the advancement of fingerprint-based access control systems and lay the foundation for future research and development in the field of biometric security.

Future scope of work

Although fingerprint door lock systems offer convenience and improved security over traditional lock mechanisms, they are not immune to vulnerabilities. Spoofing attacks, low-resolution sensors, and environmental factors can impact the accuracy and reliability of fingerprint recognition. Thus, there is a need for further advancements to strengthen the security of these systems.

Acknowledgement

We take this opportunity as a privilege to thank the Department of of Mechanical Engineering, Dr. B. C. Roy Engineering College, Durgapur-713206 for providing us absolute congenial research environment to make this project a successful one.

References

1. *Meenakshi N, Dikshit KJ, Monish M, Bharath S. Arduino based totally smart Fingerprint Authentication device. In 2019 1st global convention on innovations in facts and communique technology (ICIICT)*
2. *Moyashir R, Baidya J, Saha T, Palit R. layout and implementation of a fingerprint-primarily based key device for shared access. 2017 IEEE seventh Annual laptop and conversation conference and conference (CCWC) 2017 January 9 (pp. 1-6). IEEE.*
3. *Gupta RP. Implementation of Biometric Security in Smartphone Based Domotics. 2018 International Conference on Computer Development, Communication and Network Management (CCWC) 2018 Oct 12 (pp. 80-85). IEEE.*
4. *Islam, Md. Khayrul & Rajee, Alimul. (2022). FINGERPRINT DOOR LOCK USING ARDUINO*