Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 1, pp. 253-262
DOI : 10.47974/JIOS-1869

Development and deployment of a biometric fingerprint lock system

Shalabh Kumar Mishra [†]
Department of Electronics and Communication Engineering
Thapar Institute of Engineering and Technology
Patiala 147004
Punjab
India

Satyvir Singh [§]
Department of Mathematics
RWTH Aachen University
North Rhine-Westphalia 52062
Germany

Ashu Soni *
Akanksha Gupta [‡]
Department of Electronics and Communication Engineering
Bharati Vidyapeeth's College of Engineering
Paschim Vihar 110063
Delhi
India

Nishi Deepa Palo [@]
Saurabh Singh [#]
Charu Arora [$]
Department of Applied Sciences
Bharati Vidyapeeth's College of Engineering
Paschim Vihar 110063
Delhi
India

[†] *E-mail:* shalabhmishra14@gmail.com
[§] *E-mail:* singh@acom.rwth-aachen.de
* *E-mail:* soniashu.14@gmail.com (Corrsponding Author)
[‡] *E-mail:* akanksha.agg91@gmail.com
[@] *E-mail:* nishi.palo@bharatividyapeeth.edu
[#] *E-mail:* saurabh.singhiitbhu@gmail.com
[$] *E-mail:* charuarora099@gmail.com

Ritambhra Katoch [^]
Department of Instrumentation and Control Engineering
Bharati Vidyapeeth's College of Engineering
Paschim Vihar 110063
Delhi
India

Abstract

Security remains a paramount concern in both residential and office settings, prompting the exploration of various solutions. Existing door lock systems often exhibit vulnerabilities that compromise security, raising apprehensions about a safe lifestyle and conducive work environment. Moreover, contemporary challenges, such as terrorism and unauthorized access, underscore the urgency of implementing robust security measures, especially in shared-access spaces. This paper introduces the design and prototype of a biometric fingerprint door lock system tailored for joint access environments. Fingerprint biometrics, known for their reliability, offer a secure means to log system transactions and safeguard individual privacy rights. In contrast to RFID or password-based mechanisms susceptible to compromise, the proposed system relies solely on fingerprint verification, providing enhanced security for shared facilities. The system, built on an Arduino UNO platform, incorporates a fingerprint sensor, camera, servo motor, buzzer, and an LCD display. Authorized users' fingerprints are enrolled and verified, granting access to shared facilities, while centralized control facilitates user management. This flexible device ensures physical security by leveraging fingerprint sensor technology.

Subject Classification: *Primary 68T10, Secondary 68U10.*

Keywords: *Biometrics, Fingerprint sensor, Security system, Authorization.*

1. Introduction

In contemporary office and corporate environments, ensuring security has become a pervasive concern for individuals whether at home or away. The rapid pace of life in this competitive era makes it challenging for humans to manually safeguard their confidential belongings. Consequently, there is a growing need for automated and reliable security solutions. Common predicaments, such as getting locked out, misplacing keys, or facing theft, are a constant source of frustration for those relying on manual door locks or smart cards. To address these challenges, our fingerprint lock system offers a seamless solution. The design eliminates the need for password memorization, keys, or cards that are prone to loss.

[^] *E-mail:* `ritambhra.katoch@bharatividyapeeth.edu`

Authorized users gain swift access by simply presenting their fingerprint, ensuring a secure and efficient entry process.

Fingerprint recognition is chosen for its heightened security, as each person's fingerprint is unique. Unauthorized access is mitigated through a lock system that registers fingerprint templates of allowed users, unlocking only when a match is found. The biometric authorization leverages the unique and unchanging patterns of ridges on each fingertip, making fingerprints an unparalleled form of identification. The widespread use of fingerprint scanners in contemporary handheld devices, such as mobile phones and laptops, attests to their popularity and reliability. This paper explores the background of biometric-based lock methods in Section 2, providing insights into existing security solutions. Section 3 outlines the proposed solution, emphasizing the fingerprint method and alternative door opening mechanisms. The design and realization details of the fingerprint lock system are presented in Section 4, covering the connection diagram, software execution, fingerprint registration and deletion, and overall system functionality. Section 5 encompasses the results, including testing outcomes and user feedback. The paper concludes in Section 6 and focuses on the potential future enhancement [1-4].

2. Background

This research has examined the existing lock systems commonly employed in residences and offices. Despite their initial utility, it has been observed that over time, these methods become outdated and pose significant security risks, often accompanied by high costs. The following discussion outlines the strengths and weaknesses of prevalent lock systems [5-8].

2.1 *Password Authentication*

The analyzed system securely stores the passwords of authorized users for validation, ensuring a satisfactory level of security. However, a notable drawback is its vulnerability to unauthorized access, as malicious users can simply acquire passwords via various approaches such as hacking or guessing.

2.2 *Face Detector*

In the case of facial recognition systems, challenges arise in accurately identifying faces from images captured under diverse views and

illumination conditions. The reliability of facial recognition, solely based on facial features without contextual information, raises questions regarding its effectiveness in distinguishing individuals among many persons with high accuracy.

2.3 *Fingerprint Lock*

The fingerprint lock system, another prevalent method, offers robust security by storing and verifying the unique fingerprints of authorized users. However, it is essential to acknowledge that fingerprint identification systems may face challenges in scenarios where the quality of fingerprint images is compromised due to factors like dirt or moisture. Despite this, fingerprint systems are considered more secure and reliable compared to traditional methods [9-10].

3. Proposed Lock System

Throughout history, fingerprints have served as a reliable means of personal identification, boasting high matching accuracy. A fingerprint is effectively the inimitable pattern of ridges and valleys on the fingertip skin. Even among identical twins, fingerprints differ, highlighting the distinctiveness of everyone's prints across different fingers. Embedding fingerprint biometrics in various systems, such as laptop computers, has become economically feasible for a wide range of uses.

3.1 *Fingerprint door lock system*

The proposed fingerprint lock system stands as a dependable and highly secure solution, contributing to the enhancement of safety and convenience in various settings. This system provides a streamlined alternative, eliminating the need for users to develop complex security measures from the ground up. Additionally, we have implemented a password authentication system to enhance security measures, ensuring restricted access to individuals not enrolled in the system.

3.2 *Fingerprint Identification*

Fingerprints serve as a subset of biometrics, facilitating the identification and verification of individuals based on unique patterns. The analysis of fingerprints involves examining various features, such as aggregate characteristics like patterns and distinct minutiae points within those patterns. Both minutiae and patterns play a pivotal role in fingerprint

analysis, as no two fingers exhibit identical characteristics. The primary ridge patterns include arch, loop, and whorl: **(i) Arch:** Ridges start from one side, form an arc in the middle, and end on another side. **(ii) Loop:** Ridges start from one side, make a curve, and end on the same side and **(iii) Whorl:** Ridges form circular shape in middle of fingertip.

Fingerprint recognition systems are versatile, serving both verification (1:1 match) and identification (1:N match) purposes.

In designing the lock, simplicity was a key consideration for both the external appearance and internal components. The lock, situated beside the doorway, incorporates a fingerprint sensor, a buzzer system for user notification, and a keypad for password entry in the absence of the fingerprint bearer. An additional switch enables internal unlocking, as depicted in Fig. 1. An optical fingerprint sensor, specifically the FPM10A Fingerprint Sensor, utilizes reflective light for scanning with nearly 100% accuracy. The main items of the proposed design include Arduino Uno, fingerprint sensor, buzzer, 4x4 Matrix keypad, push button, channel relay module, electronic lock and miscellaneous items like a breadboard, wires, glue, 12V power supply, hard plastic case and a door.

As depicted in Fig. 2, the operational sequence involves placing a finger on the sensor, which reads and matches the print with the stored fingerprints. If no match is detected, the device remains inactive. Upon a successful match, it emits a single buzz and activates the electronic lock, granting access to enter inside. Along with stored fingerprints, a 4-digit password is also stored in the device. The keypad facilitates password entry, with each key press accompanied by a low beep. Upon entering the correct code, the door opens with a single buzz. Entering a wrong code results in the door remaining closed, accompanied by two beeps. After

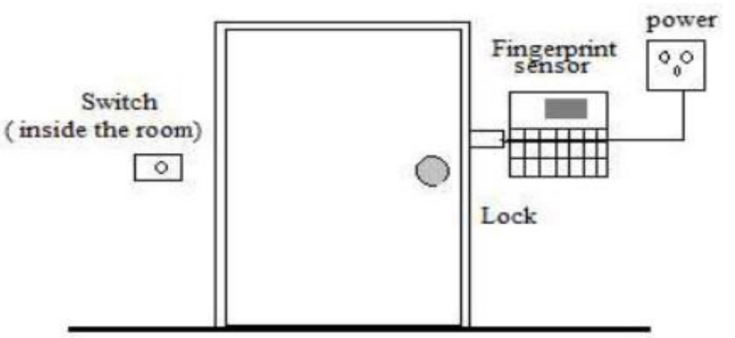

Figure 1

Conceptual representation of the fingerprint door lock system

three consecutive failed efforts, the door emits a continuous buzz for 3 seconds. A switch, located in the doorway, enables unlocking with a single buzz upon activation.

4. Design and Realization

The details of hardware and software realization are discussed in following section.

4.1 *Hardware Implementation*

After configuring the devices, we proceeded to establish the connections given in the block diagram shown in Fig. 3. The transmitter output and receiver input of the fingerprint sensor are appropriately linked to pins 2 and 3 of the Arduino. The electronic lock is linked to output port of Arduino, creating a connection with the relay to toggle between low and high supplies. The Arduino Uno is then connected to a

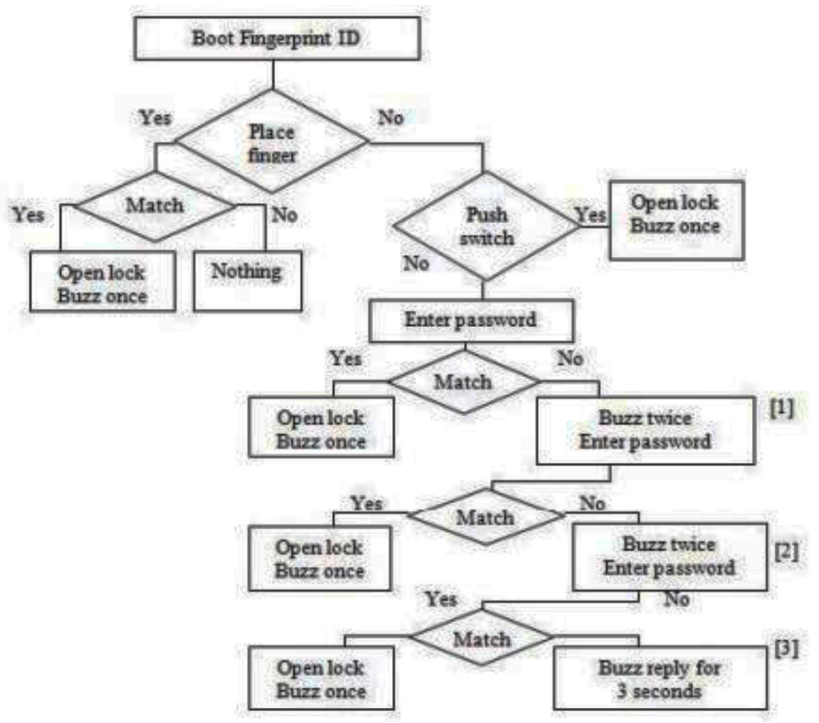

Figure 2

Flowchart of proposed design

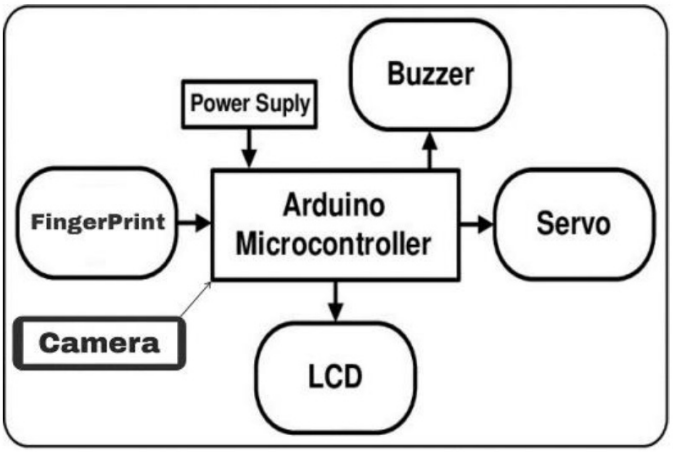

Figure 3

Connection of Arduino Microcontroller

laptop for fingerprint registration, enabling the assignment of IDs to prints. Alternatively, this connection can be facilitated through a smartphone using the Arduino application. After saving the ID into sensor and uploading the program to Arduino, we disconnected Arduino from the computer and activated the supply.

Upon powering up, the system initializes by loading the saved fingerprint IDs and awaits a print match. Keypad and switch remain active when nothing matches. Conversely, if something matches, a single buzz is emitted opening the lock. The scanner exhibits a rapid response, capable of performing over 100 scans per second, ensuring instantaneous matching when a fingerprint is placed. The system has the capacity to save 126 fingerprints, making the matching of 126 individuals' fingerprints possible.

System functionality includes enrollment of up to 126 different fingerprints for door access. Placing a registered finger results in a noise-free unlocking of the door for 5 seconds. The keypad allows entry of a 4-digit password, with each key press accompanied by a beeping sound. A correct code makes a single buzz and allows the door to open. A wrong keypad value does not allow the door to open with two buzzes. Three consecutive failed attempts on the keypad trigger a continuous 3-second buzz, signaling an unauthorized entry. Pressing switch from inner side unlocks the door for 5 seconds with one buzz.

4.2 *Software Execution*

To enroll a new fingerprint, we assembled a simple design and uploaded it to the Arduino. The following steps illustrate the fingerprint enrollment process:

a) **Fingerprint Verification Process:** To verify a registered fingerprint, finger which had been previously registered is placed against the sensor. If the Arduino successfully recognized the fingerprint, the door unlocked; otherwise, it remained locked.

b) **Fingerprint Deletion Process:** For fingerprint deletion, we input the relevant IDs into the serial monitor, initiating the deletion of the specified fingerprint.

Moreover, it is noteworthy that in the event of an incorrect PIN or an invalid fingerprint entry, the system employs a camera to capture an image. This image is then sent to the email address stored in the Arduino during the coding phase.

5. Results and discussions

To ensure the accuracy of individual components, diverse scenarios were simulated, including partial finger placement, inversion, and wet conditions. The fingerprint sensor consistently demonstrated successful matching, with a success rate exceeding 95% under normal circumstances. Notably, it struggled in extreme conditions, such as excessively dirty or oily finger, aligning with manufacturer's claim of 99% accuracy.

Additionally, the keypad was subjected to testing, where a password was entered and incorrect codes were deliberately inputted three times consecutively, yielding the expected results. The switch, a critical component in the system, underwent successful testing, unlocking the door reliably with each press. These comprehensive tests, including simulated extreme finger conditions, validate the robustness and accuracy of the fingerprint scanner, keypad, and switch functionalities.

Post-testing, the system was entrusted to a group of engineers for further examination, and their feedback was collected through a survey. The engineers affirmed the system's efficacy, and while they suggested potential enhancements, the system's current functionality was deemed reliable and secure. The universal applicability of these findings underscores the system's viability for broader implementation.

5.1 *Future Work*

The developed system exhibits considerable flexibility. While the current implementation operates with a single lock, the system's design allows for scalability by adding more electronic locks, each associated with specific fingerprint IDs through code modifications. Several potential implementations like multi-lock/decoder network system, computer based fingerprint lock system and smartphone based fingerprint security system can enhance the system's capabilities:

5.2 *Improvements*

The system's scalability permits the addition of more locks without significant cost implications. While a computer-independent system for saving prints could be explored, it would involve additional components beyond the current setup.

5.3 *Limitations*

Certain chemicals may hinder finger detection, and the system may encounter errors with dry or dirty fingers, cuts, or bruises. Additionally, the system may not be suitable for children due to the rapid changes in the size of their fingerprints. These potential implementations showcase the adaptability of the fingerprint lock system, allowing it to cater to diverse needs and environments.

6. Conclusion

The design and execution of our fingerprint lock system showcase its adaptability and cost-effectiveness. Notably, our system boasts a high accuracy rate and swift fingerprint recognition, ensuring smooth integration with users and delivering enhanced security measures. Despite its advantages, the system does have drawbacks, including its expense for a single door and dependence on electricity. Mitigating measures, such as connecting the system to an uninterrupted power supply (UPS) or incorporating rechargeable batteries, can be adopted to counteract potential power failures. In conclusion, our fingerprint lock system offers a secure solution, leveraging the uniqueness of fingerprints for reliable identification.

References

[1] A. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4-20 (2004).

[2] R. P. Wildes, "Iris recognition: an emerging biometric technology," *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1348-1363 (1997).

[3] A. K. Jain, J. Feng, and K. Nandakumar, "Fingerprint matching," *Computer*, vol. 43, no. 2, pp. 36-44 (2010).

[4] M. Lourde, and D. Khosla, "Fingerprint identification in biometric security systems," *International Journal of Computer and Electrical Engineering*, vol. 2, no. 5, 852 (2010).

[5] Z. Pala, and N. Inanc, "Smart parking applications using RFID technology," *In 2007 1st Annual RFID Eurasia*, IEEE, Turkey, pp. 1-3 (2007).

[6] M. S. Pan et al., "Fingerprint preprocessing using FCN and U-net methods," *Journal of Information and Optimization Sciences,* vol. 45, no. 5, pp. 1421-1434 (2024).

[7] R. Cappelli, D. Maio, A. Lumini and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE transactions on pattern analysis and machine intelligence*, vol. 29, no. 9, pp. 1489-1503 (2007).

[8] R. Anderson, *Security engineering: a guide to building dependable distributed systems*, John Wiley & Sons (2020).

[9] N. Begum, M. Alam and I. Islam, "Fingerprint detection based on DWT a new approach," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 14, no. 1, pp. 77-87 (2011).

[10] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 9, pp. 1489-1503 (2007).

Received August, 2024