STM JOURNALS

Journal of
Electronic Design Technology

ISSN: 2229-6980 (Online)
ISSN: 2321-4228 (Print)
Volume 16, Issue 2, 2025
May–August
DOI (Journal): 10.37591/JoEDT

https://journals.stmjournals.com/joedt

Review JoEDT

Smart Bank Locker Security System

Rahul Bhilare[1], Rohit Joshi[2]*, Vaishnavi Chandratre[3],
Supriya O. Rajankar[4]

Abstract

This paper introduces a smart bank locker security system that aims to improve the reliability and security of locker access in banks. The system has a Raspberry Pi 4B as the controller, with face detection and fingerprint scanning used for dual-factor authentication. The fingerprint scanner and facial recognition unit identify the user's identity prior to access. After successful verification, a relay is triggered to open the locker. A liquid crystal display (LCD) gives immediate feedback to users, whereas a buzzer notifies security staff in the event of unauthorized access attempts. The suggested solution provides a safe, effective, and convenient way to handle lockers. Locker security is greatly increased by using sophisticated biometric verification, which guarantees only authorized access. This creative solution, which combines technology with pragmatism to provide a highly dependable and efficient security update for personal and shared locker systems, not only improves safety but also simplifies user experience.

Keywords: Smart locker security system, Raspberry Pi 4B, biometric authentication, face and fingerprint recognition, internet of things (IoT)-based security

INTRODUCTION

Safe keeping of valuables in bank lockers has always been a fundamental banking service. The conventional locker systems based on physical keys or PINs (personal identification numbers) have proved to be vulnerable to theft, duplication, and unauthorized use [1–3]. The existing literature on the topic has ventured into using biometric systems – either face recognition or fingerprint sensors – as a better alternative compared to conventional systems. However, most of these systems use only a single layer of authentication, which in high-risk environments like banks may not be adequate. This paper proposes a smart bank locker security system that enhances security through dual biometric authentication using both face detection and fingerprint scanning, managed by a Raspberry Pi 4B [4]. This approach addresses the limitations of earlier systems by combining computer vision, biometric verification, and hardware control in a compact and cost-effective design. The scope of application of this system includes real-time user authentication, buzzer alerting, instruction on a liquid crystal display (LCD) screen, and manual control of the locker using a relay-actuated solenoid lock. The system seeks to improve the reliability, responsiveness, and usability of bank locker access with a decrease.

***Author for Correspondence**
Rohit Joshi
E-mail: rohit07joshi21@gmail.com

[1-4]Student, Department of Electronics and Telecommunication, Sinhgad College of Engineering, Pune, Maharashtra, India

Received Date: April 23, 2025
Accepted Date: May 01, 2025
Published Date: May 22, 2025

Citation: Rahul Bhilare, Rohit Joshi, Vaishnavi Chandratre, Supriya O. Rajankar. Smart Bank Locker Security System. Journal of Electronic Design Technology. 2025; 16(2): 31–36p.

LITERATURE REVIEW

Smart bank locker systems have advanced significantly with the use of biometrics and internet of things (IoT). Chikara et al. [1] led the way in fingerprint and image processing for secure access, and Baikerikar et al. [2] upgraded this with smart lock systems. Jayapriya et al. [3] further upgraded this to IoT-based remote access, further enhancing flexibility. Communication technologies such as Zigbee and GSM, as discussed by Hussain et al. [4], further enhanced system security. Giripunje et al.

[5] suggested a holistic two-way authentication method, showcasing the power of integrating biometrics with IoT in contemporary locker systems. Khairuddin et al. [6] suggested a smart security system based on Raspberry Pi with face detection and recognition, proving its suitability for access control in resource-limited environments. Likewise, Margapuri et al. [7] presented "PiBase," an IoT-based system based on Raspberry Pi and Google Firebase for real-time monitoring and alert, proving the efficacy of cloud-connected biometric security.

METHODOLOGY

System Architecture

Figure 1 shows that the smart bank locker system uses a Raspberry Pi 4B as its backbone, integrating face detection and fingerprint authentication for heightened security. A camera takes the face of the user, and it is analyzed and processed via Haar cascade classifiers. In case the face is identified, the system initiates fingerprint confirmation [8]. The fingerprint module scans and compares the entered data with retained information.

When the verification is successful, the Raspberry Pi switches on a relay to unlock the locker through a motor. Status messages are displayed on the LCD, and audio feedback is given by a buzzer. In case either check is unsuccessful, it denies access. The double-authentication system guarantees a safe and trustworthy mechanism for access to bank lockers.

Figure 2 shows the security system that begins with capturing a snapshot from a camera. Before further processing, the image is subjected to several preprocessing operations, which include noise removal, resizing, and conversion into binary and grayscale images. After preprocessing, extract salient features from the video frames in order to allow the system to effectively recognize the important facial features necessary for classification [9].

Following feature extraction, the system then uses a convolutional neural network (CNN) in an attempt to determine whether a face image is to be classified as normal or abnormal. After detecting a normal face assuming it is one previously enrolled the system will continue further and unlock the locker. However, upon presentation of an enrolled abnormal or unknown face, an alarm will be triggered, hopefully for alerting authorities or the user to a suspected intruder. The system above allows for secure real-time face access control by virtue of employing deep learning algorithms.

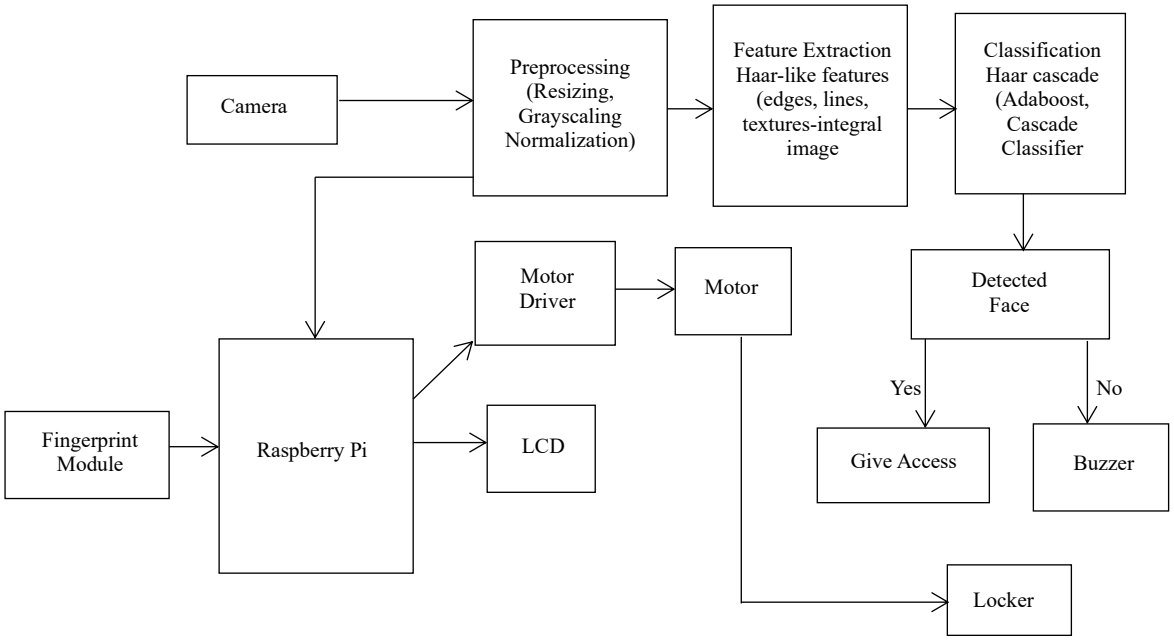

Figure 1. Block diagram of the smart bank locker security system.

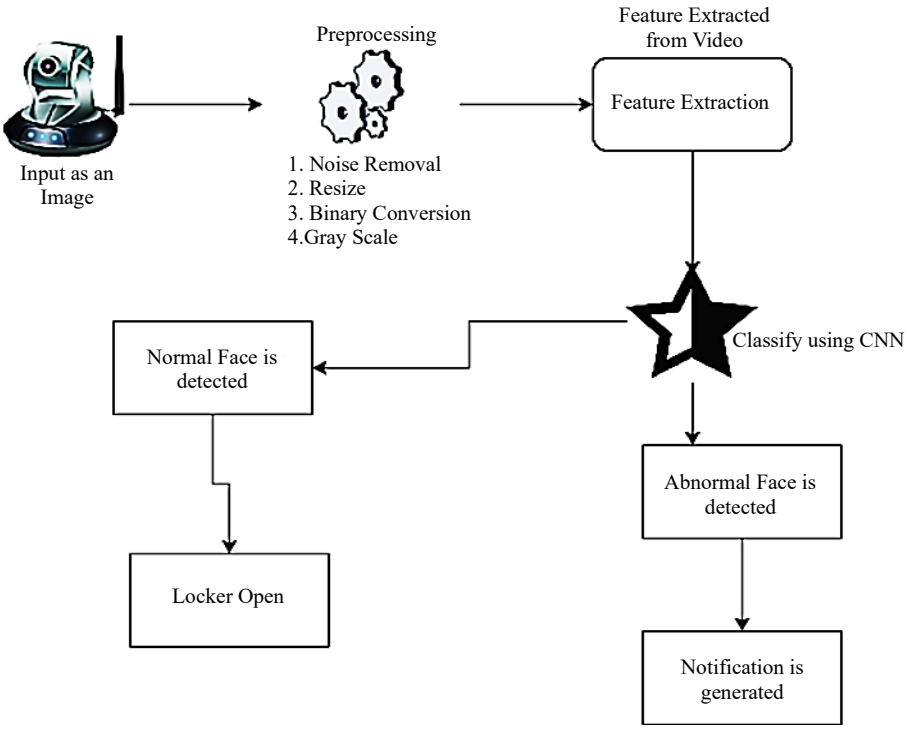

Figure 2. System architecture of the smart bank locker security system.

Hardware Implementation

1. *Raspberry Pi:* Raspberry Pi 4B is a small yet robust single-board computer featuring a 64-bit Quad-core Cortex-A72 processor operating at 1.5 GHz. It can accommodate a complete Linux OS, has 40 GPIO pins supported, USB 3.0 ports, Wi-Fi, Bluetooth, and camera interface. It is utilized here as the controller to perform biometric authentication, relay control, and email notification through Python [10].
2. *Fingerprint Module:* R307 optical fingerprint sensor is a small and effective biometric module for fingerprint identification. It captures and processes fingerprint images, digitizes them into template form, and compares them to saved templates. Through its UART (universal asynchronous receiver/transmitter) interface, it makes it easy to interface it with the Raspberry Pi. In this project, it is used as a second level verification after face recognition, thus providing an additional layer of security.
3. *Face Detection Sensor:* The Mini USB webcam is used to take real-time facial snapshots to be authenticated. Connected to the Raspberry Pi through a USB port, it cooperates with OpenCV to detect faces based on Haar cascade or deep neural network (DNN) models. In this project, it serves as the initial layer of biometric security by authenticating the face prior to fingerprint authentication.
4. *Relay:* The 5-V, 1-channel relay module is an electrical switch that permits the Raspberry Pi to switch high-voltage loads such as a solenoid lock using low-voltage signals. It is 5-V logic and gets triggered only upon successful face and fingerprint verification. The module is equipped with opto-isolation, low-level triggering, and secure connections that make it highly suitable for secure and safe operation of the locker mechanism [4].
5. *Locker:* The 12-V solenoid lock is an electromechanical device that provides the security of bank lockers. The device is driven by a 12-V DC power supply and is controlled by a relay module. The locking system provides additional security after the successful execution of both biometric authentication processes.
6. *Buzzer:* The buzzer in the intelligent bank locker system is a critical sound warning device, driven by a 5-V direct current and controlled by the microcontroller. It provides instant audio feedback on events like results of biometric verification, unauthorized access attempts, and changes in system status, thus complementing security measures as well as user alertness.

Software Implementation

1. *Proteus 8 Professional:* Proteus 8 Professional was employed to simulate and design the electronic circuits of the system. The software allowed the testing of devices like microcontrollers, sensors, and relays in a virtual environment prior to physical implementation.
2. *OpenCV:* The system integration with OpenCV was done in order to carry out computer vision processes, that is, facial detection for the intention of biometric authentication. OpenCV is a large, open-source library offering considerable functionality in the processing of real-time videos and images.
3. *Python 3 IDE:* The control flow and application logic of the system were developed in Python 3 and a Python integrated development environment (IDE). Python was chosen because it is easy to learn, easy to use, and has good support libraries. The Python IDE provided an easy-to-use environment for coding, testing, and debugging [3].
4. *SQLite:* SQLite was utilized as the local database engine for data storage and management. SQLite held data, biometric templates, access logs, and system events

Algorithm

Haar cascade is an object detection technique employed to detect objects such as faces, eyes, and hands in images and videos [11]. It is a machine learning-based technique proposed by Viola and Jones in 2001 and is commonly employed in OpenCV for real-time face detection

1. *Haar-like Features:* Haar features are employed in object detection to identify image contrasts and act like edge detection filters. They examine differences in pixel luminance across neighboring areas. Edge features (light-dark edges), line features (horizontal or vertical features), and four-rectangle features (employed to detect facial features such as eyes, nose, and mouth) are common.
2. *Integral Image Calculation:* The integral image approach allows for efficient computation of the feature values. Instead of computing pixel values one by one, an integral image allows for region sums to be computed in constant time.
   Formula for Integral Image (l (x, y))

   $$I(x, y) = I(x, y - 1) + I(x - 1, y) – I(x - 1, y - 1) + f(x, y)$$

3. *AdaBoost Training:* As not all Haar features contribute equally to the accuracy of detection, the most helpful ones are chosen by the AdaBoost algorithm. The features are given weights and the weights are updated iteratively while learning to focus more on the better ones. These features are used to train weak classifiers, which are boosted and combined together to get the final strong classifier.
4. *Cascade Classifier:* The Cascade classifier enhances detection speed through a serial sequence of stages, as opposed to employing all features at once. The image is scanned at different stages, and if at any stage a certain region fails to meet the requirements, it is eliminated immediately.

IMPLEMENTATION AND RESULT

Testing

The system was tested with valid and invalid face and fingerprint inputs to verify proper authentication. It always granted access only on valid matches, triggered alarms on failures, and showed quick, consistent performance is shown in Table 1.

Table 1. Testing table.

Test Case	Face match	Fingerprint Match	Result	Unlock
TC1	Yes	Yes	Success	Yes
TC2	Yes	No	Failed	No
TC3	No	Yes/No	Failed	No
TC4	No	No	Failed	No
TC5	Yes	Yes	Success	Yes

Evaluation Parameter

1. *Accuracy:* Percentage of successful authentications using face and fingerprint.
2. *False Acceptance Rate (FAR):* FAR rate of unauthorized users incorrectly granted access.
3. *False Rejection Rate (FRR):* Rate of valid users incorrectly denied access.
4. *Authentication Time:* Time taken to complete both authentication steps.
5. *Response Time:* Delay between authentication and locker activation.
6. *Power Efficiency:* Low power performance on Raspberry Pi 4B hardware.
7. *Alert Response:* Buzzer response to wrong access attempts.

Test Result Table

Table 2 shows the final results of the proposed system.

1. Face detection accuracy: 94%
2. Fingerprint accuracy: 94%
3. Overall system accuracy: 93%
4. FAR (false acceptance rate): 0%

Graph

Figure 3 shows the system performance for five users. Face and fingerprint recognition were 100% accurate, and most users could access the locker. Small dips in biometric accuracy marginally raised failed attempts, dictating the system's overall reliability.

Table 2. Result table.

User ID	Face Detection Accuracy	Fingerprint Accuracy	Total Attempts	Successful Access	Failed Accesses
U1	100%	100%	5	5	0
U2	100%	80%	5	4	1
U3	90%	90%	5	4	1
U4	80%	100%	5	4	1
U5	100%	100%	5	5	0

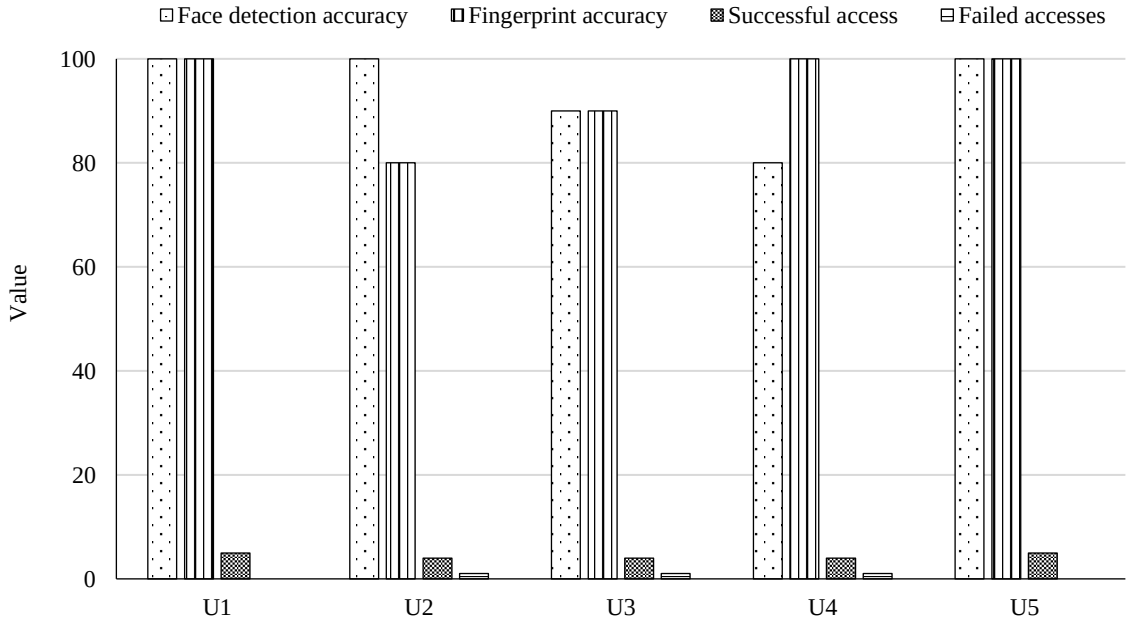

Figure 3. Graph of the smart bank security system.

Interpretation of Result

The interface of the system displays the outcome of the biometric verification both by way of face detection and fingerprint identification. In case of successful instances, both "Face Authenticated Successfully." and "Fingerprint Authenticated Successfully" are recognized by way of the GUI (graphical user interface), indicating accurate user identity and grant of access [4]. In cases where the fingerprint cannot be verified but the face is recognized, access is denied, and the GUI displays "Oops!!! Fingerprint Not Authenticated." In cases where the face cannot be verified but the fingerprint is recognized, access is denied, and the GUI displays "Oops!!! Face Not Authenticated." This feedback confirms that security permits entry only when the biometric parameters have been verified, for the reasons of enhanced dependability and lowered illegal access.

CONCLUSIONS

The proposed smart bank locker security system effectively combines biometric authentication with real-time management capabilities facilitated by the Raspberry Pi 4B. With facial recognition combined with fingerprint authentication, the system ensures a two-layer security system, minimizing the possibility of unauthorized access. In addition, the employment of a relay system for locker control and a buzzer for alert notification enhances both effectiveness and security features. The affordable and scalable solution is very promising for the transformation of traditional locker systems for banking organizations into a secure and easy-to-use alternative.

REFERENCES

1. Chikara A, Choudekar P, Ruchira, Asija D. Smart bank locker using fingerprint scanning and image processing. In: 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, March 6–7, 2020. pp. 725–728.
2. Baikerikar J, Kavathekar V, Ghavate N, Sawant R, Madan K. Smart door locking mechanism. In: 2021 4th Biennial International Conference on Nascent Technologies in Engineering (ICNTE), Navi Mumbai, India, January 15–16, 2021. pp. 1–4.
3. Jayapriya J, Arulmozhi M, Jagadeesh V, Sandhiya M, Ali AN. Enhancing bank locker security through multi-layered authentication and IoT integration. In: 2024 IEEE Recent Advances in Intelligent Computational Systems (RAICS), Kothamangalam, Kerala, India, May 16–18, 2024. pp. 1–6.
4. Hussain AF, Ajaz F, Ahmed N, Stephen H, Li Y, Mujib AM, Arshad J, Das PK. Zigbee and GSM based security system for business places. In: 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, March 4–5, 2021. pp. 264–267.
5. Giripunje LM, Sudke S, Wadkar P, Ambure K. IOT based smart bank locker security system. Int J Adv Res Sci Eng Technol. 2018; 7 (Spl Issue 3): 884–891.
6. Khairuddin MH, Shahbudin S, Kassim M. A smart building security system with intelligent face detection and recognition. IOP Conf Ser Mater Sci Eng. 2021; 1176 (1): 012030.
7. Margapuri V, Penumajji N, Neilsen M. PiBase: An IoT-based security system using Raspberry Pi and Google Firebase. arXiv preprint. arXiv:2107.14325. July 29, 2021.
8. Jadhav SH, Agrawal SS. Smart bank locker security system using biometric fingerprint and GSM technology. Int J Sci Res. 2016; 5 (10): 1920–1925.
9. Vadukanathan A, Duraikannu G, Jaganathan V, Sridhar S, Suyambrakasam G. Enhanced bank locker security system utilizing RFID for dual-layer protection. In: 2024 5th International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, September 18–20, 2024. pp. 283–288.
10. Mahendra S, Sathiyanarayanan M, Vasu RB. Smart security system for businesses using internet of things (IoT). In: 2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT), Bangalore, India, August 16–18, 2018. pp. 424–429.
11. Naveen P, Teja MS, Kalyan KP, Basha SM. Bank locker security system using QR code. Ann Romanian Soc Cell Biol. 2021; 25 (5): 4218–4227.

