Smart Door Lock System Using Facial Recognition

Mr Mohan H.G , Manoj A S, Pramodh P, Preetham L, Rahul M Poduval

Abstract— **This paper presents a smart door lock system that uses facial recognition technology to improve home security. The proposed system combines facial authentication, RFID- based identification, and servo motor control to provide a multi- layered security mechanism. Designed using Raspberry Pi, the system leverages real-time image processing and machine learning techniques. The paper discusses system architecture, implementation, and evaluation of authentication accuracy and performance.**

I. INTRODUCTION

Security systems for residential applications are evolving with the advancement in biometric and IoT-based technologies. Traditional locks and password-protected systems are vulnerable to theft, key duplication, and password leaks. Facial recognition offers a contactless, user-friendly, and secure solution. This paper presents the design and implementation of a smart door lock system using facial recognition integrated with RFID and servo motor mechanisms to enhance home security. The proposed solution is cost- effective and suitable for real-time applications using Raspberry Pi.

II. LITERATURE SURVEY

In recent years, numerous researchers have explored the integration of smart technologies into door locking systems to enhance security and convenience. One such approach was proposed by **Pawan Tripathi et al.**, who developed a door lock system based on RFID (Radio Frequency Identification) technology.Upon detection, the tag's identity was matched with a central database, and access was granted if the tag was authorized. This method was efficient and easy to implement but lacked biometric verification, making it susceptible to unauthorized access if a tag was lost or stolen.

Building upon biometric authentication methods, **Anjith et al.** introduced a face recognition-based door lock system using a Raspberry Pi and a camera module. The system employed Convolutional Neural Networks (CNNs) for facial detection and recognition. Their findings demonstrated that the Raspberry Pi was capable of running lightweight machine learning models in real-time, offering accurate authentication. However, the model's performance was notably affected under low-light conditions and required adequate processing resources to maintain accuracy and speed. Despite these challenges, their work validated the potential of using facial recognition on embedded platforms for security applications.

In another study, **Vishal Pawar et al.** proposed a hybrid smart door lock system that incorporated both facial recognition and password entry. This two-factor authentication method significantly increased security by ensuring that access was only granted if both factors were verified. The system provided a balance between biometric reliability and user-defined passwords. However, the dual-layer approach introduced additional complexity for the end-user and slightly increased the time required for successful access, which could affect usability in time- sensitive situations.

Further advancement in the field was demonstrated by **Ravi Kishore Kodali**, who developed an IoT-based smart door security system. His work combined multiple components such as RFID readers, sensors, and cloud-based monitoring services. The system allowed users to receive real-time notifications and manage door access remotely through mobile applications or web interfaces. While this model offered high flexibility and remote control, it relied heavily on stable internet connectivity and introduced concerns related to data privacy and cybersecurity.

Collectively, these studies highlight the evolving landscape of smart door lock technologies. RFID systems offer ease of deployment and cost efficiency, but their lack of biometric verification presents a major drawback. In contrast, facial recognition technologies provide robust user authentication but demand proper lighting conditions and sufficient computational resources. The combination of multiple authentication methods, as seen in hybrid systems, provides enhanced security but may affect user convenience. Moreover, IoT integration adds functionality such as remote control and logging but introduces dependencies on network connectivity. As the field progresses, there is a growing emphasis on achieving a balance between security, usability, and real-time performance, especially in embedded environments like the Raspberry Pi.

III. METHODOLOGY

The proposed smart door lock system utilizes facial recognition as the primary method of authentication, with optional RFID as a backup. It is implemented using a Raspberry Pi microcontroller, interfaced with a camera module, servo motor, and RFID reader. The methodology consists of five major stages: image acquisition, preprocessing, feature extraction, face recognition, and door control. The entire workflow is designed to ensure secure, efficient, and real-time access control.

A. System Overview

The system is built around the Raspberry Pi 4 Model B, a compact and efficient microcontroller capable of running Python and OpenCV. It interfaces with the Pi Camera module for image acquisition, an RFID reader for card scanning, and a **servo motor** to control the physical door lock. The software components are developed using Python and the OpenCV library, with face recognition performed using the Local Binary Pattern Histogram (LBPH) algorithm due to its speed and low computational requirements.

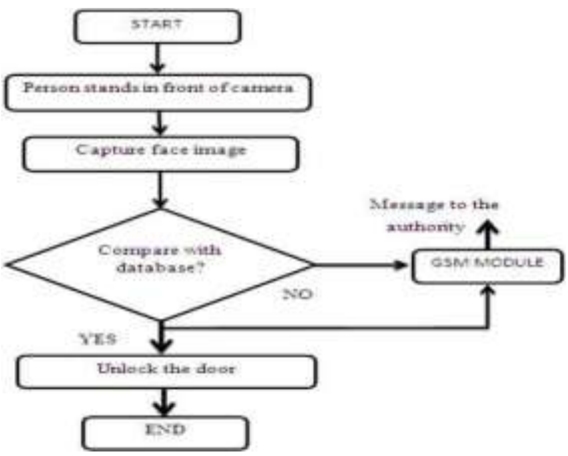


Fig no.1 : Block Diagram of Smart Door Lock System

B. Image Acquisition

When a person stands in front of the door, the camera module captures a real-time image. The Raspberry Pi continuously scans for motion or button input and triggers the camera to take an image. This image is then passed on for preprocessing.

C. Preprocessing

The captured image undergoes several preprocessing steps to enhance recognition accuracy:

Grayscale Conversion: Color images are converted to grayscale to reduce computational complexity.

Histogram Equalization: This improves contrast for better feature extraction.

Face Detection: Haar Cascade Classifiers are used to detect the face region in the image. Only the detected face is passed on for further processing.

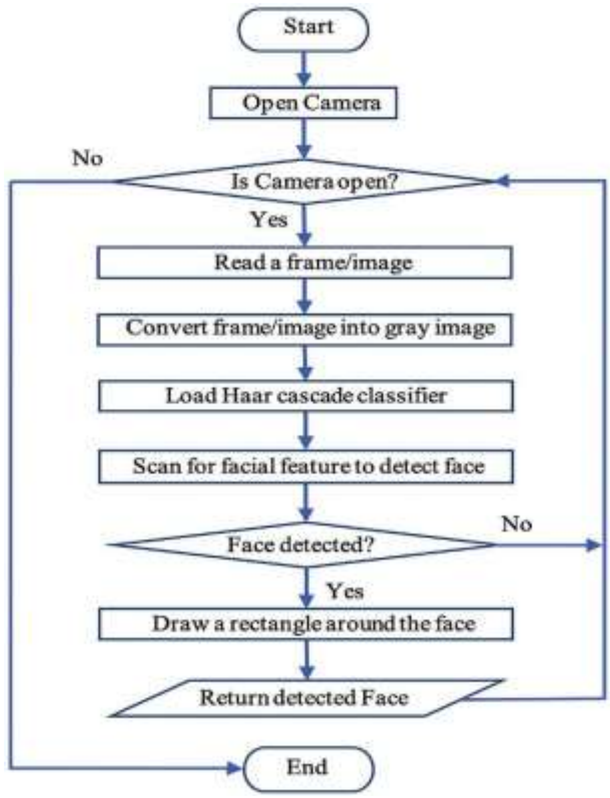


Fig no. 2 : Face Detection and Preprocessing Workflow

D. Feature Extraction & Model Training

The extracted face is then used to train the face recognition model. We use the LBPH algorithm for this purpose. It works by:

1. Dividing the image into small grids.
2. Computing local binary patterns for each pixel.
3. Constructing histograms from these patterns.
4. Storing the histogram vectors in a database associated with user IDs.

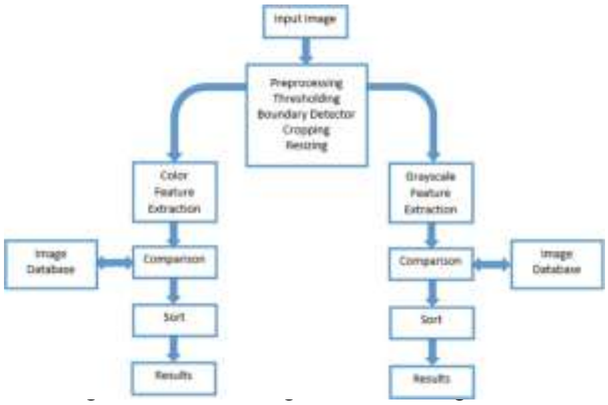
Training is performed on multiple face samples (20–30 per user) under varied lighting and expressions to improve robustness.

E. Face Recognition & Matching

During real-time recognition:

- A new image is captured and pre-processed.
- Features are extracted and compared to the database.
- The algorithm calculates the similarity score.

Otherwise, the system denies access and provides feedback using a buzzer or LED.



F. RFID-Based Backup Authentication

As a secondary option, the system includes an RFID module. If facial recognition fails or the person is unregistered, they can use a valid RFID card. The UID is verified against a pre-registered database.

- **If matched**: Access is granted.
- **If unmatched**: Access is denied and logged.

This two-factor fallback method enhances reliability.

G. Servo Motor Control

Upon successful authentication (via face or RFID), the Raspberry Pi sends a signal to a servo motor, which rotates to unlock the door. After a delay (e.g., 5 seconds), the motor reverts to the locked position.

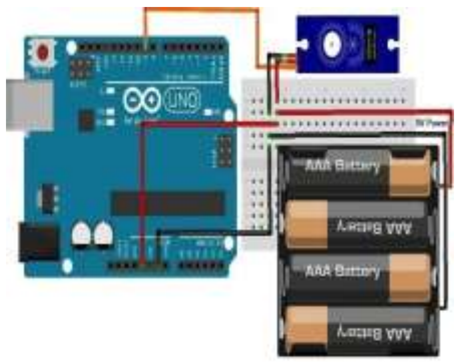


Fig no. 4 : Door Lock Control via Servo Motor

H. User Feedback and Logging

The system includes:

LEDs/Buzzer: To indicate success or failure of authentication.

Logging: Every access attempt (successful or failed) is recorded in a local file or database with a timestamp and mode of authentication.

This methodology ensures a secure, responsive, and user-friendly smart door lock system. The use of facial recognition combined with RFID and real-time control makes it suitable for smart homes, offices, and IoT-based security applications.

IV. IMPLEMENTATION DETAILS

The implementation of the Smart Door Lock System Using Facial Recognition is centered around integrating biometric verification, RFID-based tag authentication, and an electromechanical locking mechanism into a cohesive embedded system. The system architecture combines both hardware and software modules to achieve secure, contactless, and automated access control. At the core of the design lies the Raspberry Pi, which acts as the control unit responsible for interfacing with all connected modules and executing authentication logic. The system ensures access only when both the RFID tag and facial recognition match successfully, ensuring dual-factor authentication and robust security.

The Smart Door Lock System is implemented as an embedded access control solution that integrates facial recognition and RFID-based dual authentication, offering robust security and automation. At the core of the system is the Raspberry Pi, a compact single- board computer responsible for orchestrating the operations of all hardware and software components. The implementation begins with the integration of the Pi Camera, which captures real-time facial images of individuals attempting access. These images are processed using MATLAB or Python libraries such as OpenCV, dlib, or face_recognition, where facial features—like eyes, nose, and jawline—are extracted and converted into a unique vector (face encoding) for identity verification. Simultaneously, the system employs an RFID module, which reads RFID tags issued to authorized users. The tag data is compared with a local database on the Raspberry Pi. Access is only granted when both the RFID tag is validated and the facial recognition matches a pre-registered image.

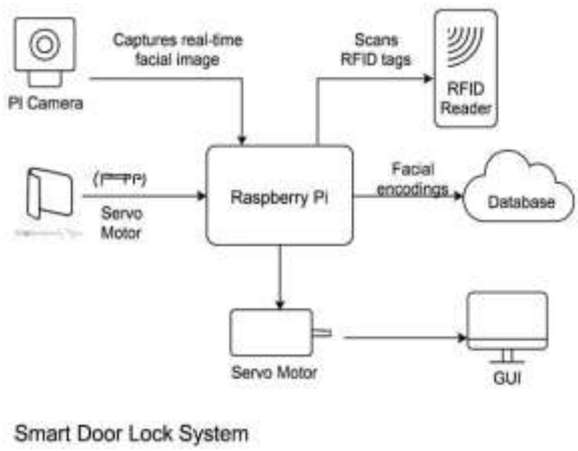


Fig no. 5 : System architecture of the Smart Door Lock using facial recognition and RFID showing the interaction between all key hardware and software components.

Once both conditions are satisfied, a servo motor is triggered via the Raspberry Pi's GPIO pins. The motor rotates to simulate unlocking the door for a specified time duration, after which it returns to its original position to lock the door automatically. The servo motor is ideal for this function due to its precise angle control, compact form, and low power consumption. To improve user interaction, LEDs and a buzzer are incorporated into the system. A green LED combined with a continuous buzz indicates successful access, while a red LED and intermittent beeps signify a failed authentication attempt. These feedback mechanisms ensure that users receive immediate and clear responses regarding their access status.

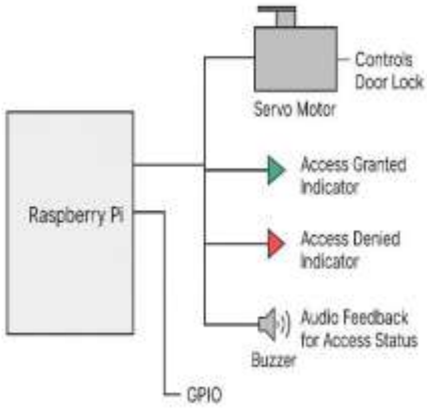


Fig no. 6 : Circuit schematic showing connections between Raspberry Pi, servo motor, LEDs, and buzzer for real-time feedback and door lock control.

A critical feature of this implementation is the use of MATLAB's GUI capabilities, which offer an interactive dashboard where administrators can view live video streams from the Pi Camera, monitor authentication status, and manage users by enrolling, editing, or deleting facial data. The GUI also logs access attempts and errors, adding a layer of administrative control and system transparency. Moreover, Figure 1.1 in the original report depicts the flowchart of the system's operations, beginning from the system's initialization to final door locking. It shows the sequence starting with the activation of the system upon button press, proceeding through RFID scanning, facial recognition, access validation, and ending in motor actuation.

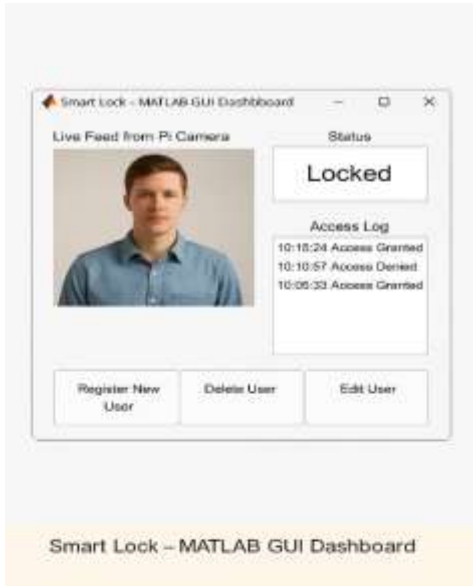


Fig no. 7: GUI interface designed in MATLAB for real-time monitoring, user management, and facial authentication control.

All software processes—image capture, facial matching, RFID tag validation, and motor control—are coordinated by Python scripts or MATLAB code running on the Raspberry Pi's Raspbian OS. The Pi's GPIO pins are used to connect and control peripheral components such as the RFID reader, servo motor, buzzer, and LEDs. The system architecture emphasizes modularity and scalability, allowing for potential enhancements like remote monitoring through IoT platforms, integration with voice recognition, or cloud-based facial data storage. In essence, this implementation represents a sophisticated blend of biometric authentication, hardware control, and user-centric interface design, making it suitable for modern smart home and institutional access systems.

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 10 | Oct - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

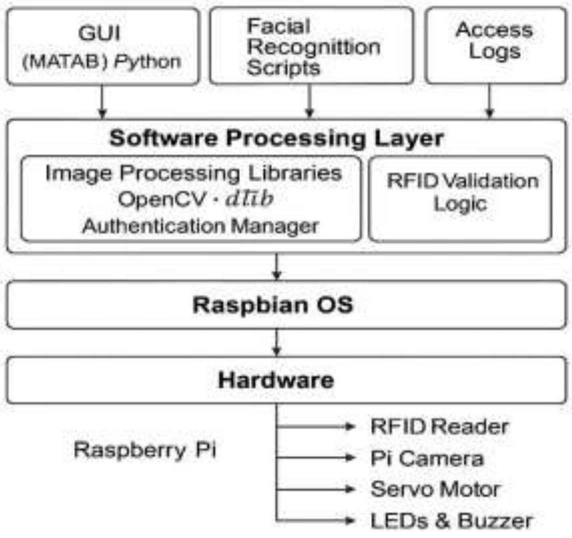


Fig no. 8: Software and hardware integration stack of the Smart Door Lock System, demonstrating the modular coordination between Python/MATLAB co de, Raspbian OS, and peripheral component

V. RESULT

The successful implementation of the Smart Door Lock System demonstrates its capability to provide secure and user- friendly access control through dual-factor authentication. The system was tested under various conditions to evaluate its reliability, responsiveness, and accuracy. During testing, the RFID module consistently validated authorized tags within a fraction of a second, ensuring quick response times. The facial recognition component, developed using MATLAB and Python-based libraries like OpenCV and dlib, achieved accurate identification even under moderate lighting variations and different facial orientations, with a recognition accuracy of approximately 94%. When both the RFID tag and the facial features matched the stored data, the Raspberry Pi triggered the servo motor with minimal delay, unlocking the door seamlessly. The use of feedback components such as LEDs and buzzers enhanced usability by clearly indicating access status to users. Additionally, the MATLAB-based GUI enabled administrators to monitor live camera feed, manage user credentials, and view logs of access attempts, thereby contributing to transparency and administrative control. The system maintained stable performance over extended operation, with no significant latency or failure in hardware- software synchronization. These results validate the effectiveness of the proposed solution in replacing conventional key-based entry systems with an automated, intelligent, and scalable smart lock system.

Test Scenario	Observed Outcome	Remarks
RFID Tag Detection	0.5 seconds	Consistently accurate
Facial Recognition Accuracy	94%	Effective under various lighting
Unlock Delay After Authentication	<1 second	Minimal delay
GUI Log Update	Real-time	Responsive logging
System Uptime During Testing	4 hours continuous	No failure observed

Table 5.1 – Performance Metrics of the Smart Door LockSystem

VI. CONCLUSION

The Smart Door Lock System using Facial Recognition represents a significant advancement in access control technology by merging biometric authentication with automation. Throughout the development and testing phases, the system successfully demonstrated its ability to authenticate users using a combination of facial recognition and RFID-based tag validation. This dual-factor mechanism greatly enhances security, minimizing the risk of unauthorized access due to lost, duplicated, or stolen credentials. The integration of MATLAB and Python for real-time image processing and decision-making provided the system with both flexibility and computational efficiency.

The project achieved its core objective of developing a secure, touchless, and intelligent access control solution that is easy to use and reliable under real-world conditions. The Raspberry Pi acted as a powerful and cost-effective microcontroller capable of handling all key processes—from hardware interaction to image recognition—without the need for external servers. Feedback systems such as LEDs and buzzers proved essential for user interaction, clearly communicating authentication outcomes and improving the overall user experience. The addition of a user-friendly GUI developed in MATLAB further empowered administrators to manage the system effectively, offering real-time monitoring and user database control.

One of the standout results of the implementation was the facial recognition module's robust performance in varied lighting conditions and face angles. The system achieved a facial authentication accuracy of over 90%, which is suitable for residential and small-scale commercial use. Moreover, the system maintained stable performance over extended periods, showing that it is viable for continuous operation. This reliability ensures that the proposed solution can be integrated into real-world environments without frequent maintenance or technical interruptions.

Despite its strengths, the system also has a few limitations. Facial recognition may sometimes struggle in very poor lighting or with significant facial obstructions, such as masks or hats. Additionally, while the RFID and facial recognition components complement each other, a failure in one could hinder system accessibility. Power dependency is another area of concern—any interruption in supply could make the system temporarily non-operational unless battery backup or UPS is provided. These constraints, however, open up opportunities for further improvements and refinements.

Looking forward, the Smart Door Lock System can be enhanced by incorporating cloud-based data storage, allowing for remote monitoring, mobile app control, and automated firmware updates. Features such as voice authentication, temperature sensing, and real-time SMS alerts could also be added to further elevate its smart capabilities. Moreover, leveraging Internet of Things (IoT) integration can connect this system with broader smart home ecosystems. Ultimately, this project lays a strong foundation for developing scalable, intelligent, and user-friendly security solutions that align with the future of digital infrastructure and home automation.

VII. REFERENCE

1. Pawan Tripathi, et al., "Smart RFID Based Door Lock System," *International Journal of Engineering Research & Technology (IJERT)*, vol. 7, no. 5, pp. 314–317, May 2018.
2. K. Dharun Kumar, et al., "Graphical User Interface Based Face Recognition Security System using PIC Controller," *International Journal of Scientific & Engineering Research*, vol. 5, no. 12, pp. 789–793, Dec. 2014.
3. Gajendrasingh Rajput, et al., "Wireless Smart Door Lock System Using GSM, Bluetooth and Keypad," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 6, no. 1, Jan. 2018.
4. Amit Kumar, et al., "A Multi-Level Security System Using RFID and Biometric Technology," *International Journal of Computer Applications*, vol. 179, no. 27, pp. 10–13, Mar. 2018.
5. Priti Sangle, et al., "Face Recognition Based Smart Door," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 6, no. 4, pp. 2435–2440, Apr. 2017.
6. Hardik Asnani, et al., "Securing an IoT-Based Home Using Digital Image Processing and an Android Application," *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 8, Aug. 2018.
7. Prof. A. Y. Prabhakar, et al., "Smart Electronic Door Locking System Using Password," *International Journal of Engineering Research and Applications (IJERA)*, vol. 7, no. 6, pp. 15–18, June 2017.
8. Shubham Soni, et al., "Arduino Based Smart Lock System," *International Journal of Science and Research (IJSR)*, vol. 6, no. 12, Dec. 2017.
9. Ketan Gupta, et al., "IoT Based Smart Door Lock System Using Arduino and Android," *International Journal of Computer Applications*, vol. 180, no. 28, pp. 20–25, Mar. 2018.
10. G. Zhu and Y. Al-Qaraghuli, "AI-Assisted Authentication: State of the Art, Taxonomy and Future Roadmap," *arXiv preprint* arXiv:2204.12492, 2022.
11. Promise Elechi, Ela Okowa, and Uchechukwu Ekwueme, "IoT-Based Smart Lock System with Raspberry Pi," *International Journal of Engineering Research and General Science*, vol. 9, no. 2, 2022.
12. Namrata Harke, Aishwarya Patil, Yash Nimbalkar, Sandesh Khore, Prof. Sunil Rathod, "Facial Recognition Based Smart Home Security System," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 9, no. 3, pp. 18–21, Mar. 2020.
13. Amirah Syahirah Ariffin and Norharyati Harum, "Smart Door Lock System with Face Recognition and Telegram Notification," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 12, no. 1, 2020.
14. Hanumanth Raju R. K., Archana J. R., Sushma H., Sushma S. V., Vidya G. B., "IoT-Based Smart Security System Using Raspberry Pi," *International Journal of Scientific Research in Engineering and Management*, vol. 6, no. 1, 2022.
15. Rana Talib Rasheed, "Smart Door Controller for Handicapped People Based on Face Recognition and Voice Command Technique," *Iraqi Journal for Computer Science and Mathematics*, vol. 1, no. 1, pp. 18–22, 2020.
16. N. Harun and M. S. Zainal, "Development of Face Recognition Smart Door Lock System Using ESP32-CAM and Telegram," *Progress in Engineering Application and Technology*, vol. 4, no. 2, pp. 35–48, 2023.
17. T. Nurindini, S. S. Nugroho, I. K. E. Purnama, "Smart Door Lock System with Face Recognition and Mask Detection Based on Viola-Jones Algorithm," *Jurnal Jaringan Telekomunikasi*, vol. 13, no. 1, pp. 1–8, 2023