

INTELLIGENT LAYERED SMART DOOR LOCK SYSTEM USING RASPBERRY PI

19EEE381-OPEN LAB

Report

*Submitted b*y

CB.EN.U4ELC22012 GOPIKRISHNA K

CB.EN.U4ELC22014 HARIKRISHNAN MIRAJ

CB.EN.U4ELC22015 JAISRIHARI G

CB.EN.U4ELC22063 NANDAN RAJESH

DEPARTMENT OF ELECTRICAL AND ELECTRONICS ENGINEERING

AMRITA SCHOOL OF ENGINEERING,

AMRITA VISHWA VIDYAPEETHAM,

COIMBATORE - 641112

March and 2025

**Amrita School of Engineering**

**Department of Electrical and Electronics Engineering**

**Program Educational Objectives (PEOs)**

**PEO1:**Graduate can demonstrate electrical and electronics engineering problem solving skill along with proficiency in communication and professional excellence in project management and execution.

**PEO2:**Graduate can be employable in engineering services including ICT enabled sectors and also motivated for entrepreneurship.

**PEO3:**Graduate will be competent for higher studies in world class universities and research in industrial organizations.

**PEO4:**Graduate will manifest social commitment, environmental awareness and moral and ethical values in professional and other discourses.

**Program Specific Outcomes (PSOs)**

**PSO1:** Build and manage electro dynamic systems using Knowledge on electrical technology and semiconductor devices for allied services.

**PSO2:** Use computational tools and network dynamics for design, analysis and control of power systems integrated with renewable energy and Electric Vehicle.

**PSO3:** Leverage digital technologies employing state-of- the art control techniques and embedded controllers for industrial applications.



BONAFIDE CERTIFICATE

This is to certify that the open lab project report entitled “Intelligent Layered Smart Door Lock using Raspberry Pi”,

submitted by

Roll Nos. Student Names

CB.EN.U4ELC22012 GOPIKRISHNA K

CB.EN.U4ELC22014 HARIKRISHNAN MIRAJ

CB.EN.U4ELC22015 JAISRIHARI G

CB.EN.U4ELC22063 NANDAN RAJESH

is in partial fulfillment of the requirements for the award of the **Degree of** **Bachelo**r **of Technology** in **“Electrical and Electronics Engineering”** is a bonafide record of the work carried out at Amrita School of Engineering, Coimbatore.

Internal Examiner External Examiner

**CONTENTS**

Sl. No. List of Contents Page No.

1. ABSTRACT 5
2. INTRODUCTION 6
3. PROBLEM STATEMENT 7
4. METHODOLOGY 8
5. RESULTS 10
6. CONCLUSION AND FUTURE WORK 12
7. REFERENCES 14

###### ABSTRACT

With the increasing need for security in residential and commercial environments, automated access control systems have become essential. This project presents a Smart Door Lock System using Raspberry Pi, Pi Camera, Histogram of Oriented Gradients (HOG)-based face recognition, OTP authentication, an ultrasonic sensor, and a GSM[5] module to provide a secure and automated access mechanism. The system is designed to enhance security through multi-layered authentication, ensuring only authorized individuals can gain entry while also alerting the owner in case of unauthorized access attempts.

The primary mode of authentication in this system is face recognition[2], which employs the HOG algorithm for feature extraction and face encoding using the “face\_recognition” library. When a person approaches the door, an ultrasonic sensor detects their presence and triggers the Pi Camera to capture an image. The captured face is then compared against a pre-trained dataset of authorized users. If the system recognizes the individual with a confidence score above a set threshold, it activates a relay-controlled solenoid lock to grant access.

If face recognition[2] fails after multiple attempts, the system initiates OTP-based authentication as a secondary security measure. A randomly generated 4-digit OTP is sent to the registered mobile number via a GSM[5] module, and the user must enter the correct OTP using a 4x4 matrix keypad[6] to unlock the door. If incorrect OTPs are entered multiple times, the system activates an intruder alert mechanism, sending an SMS warning to the owner, triggering a buzzer, and initiating a security lockdown. Additionally, the system features LED indicators to provide real-time authentication feedback, with green indicating successful authentication and red signaling an unauthorized attempt.

This smart door lock system provides an efficient, cost-effective, and scalable security solution that integrates biometric authentication and mobile-based verification to enhance safety. By combining HOG-based face recognition, OTP authentication, and real-time monitoring, the system ensures high reliability and protection against unauthorized access. Designed for modern homes, offices, and high-security zones, this project contributes to the advancement of automated security technology, offering a seamless, user-friendly experience while maintaining robust access control.

###### INTRODUCTION

In today’s world, security is a major concern in both residential and commercial environments. Traditional locking mechanisms, such as mechanical keys and numeric keypads[6], are prone to vulnerabilities, including key duplication, unauthorized access, and forgotten passwords. As a result, the need for advanced and automated access control systems has significantly increased. Biometric authentication, particularly face recognition[2], has emerged as a reliable and user-friendly alternative for enhancing security. This project aims to develop a Smart Door Lock System using Raspberry Pi[1], Pi Camera, Histogram of Oriented Gradients (HOG)-based face recognition, an ultrasonic sensor, and OTP-based authentication to provide a robust and multi-layered security mechanism.

The system is designed to automate door access by verifying the identity of an individual using face recognition[2]. When a person approaches the door, an ultrasonic sensor detects their presence and activates the Pi Camera to capture an image. The system then processes the image using the HOG algorithm, extracts facial features, and compares them with pre-stored encodings of authorized users. If a match is found, the door is unlocked using a relay-controlled solenoid lock. This ensures that only registered individuals can gain access without the need for physical keys or PIN codes.

To further enhance security, the system incorporates an OTP-based verification mechanism as a secondary authentication method. If face recognition fails after multiple attempts, a one-time password (OTP) is sent to the registered user’s mobile phone via a GSM[5] module. The user must enter the correct OTP using a 4x4 matrix keypad[6] to gain access. If multiple incorrect OTPs are entered, the system activates an intruder alert, sending a warning message to the owner, triggering a buzzer and alerting the homeowner and the neighbours around, and preventing further attempts.

The LED indicators provide real-time feedback on authentication status, with a green LED signalling successful verification, a red LED and a buzzer indicating an unauthorized attempt. Additionally, the system logs access attempts, allowing for better monitoring and security management.

This project demonstrates how biometric authentication and mobile-based verification can be combined to create a highly secure and automated access control system. The implementation of HOG-based face recognition ensures efficient processing while maintaining high accuracy in detecting and verifying faces. Furthermore, the integration of OTP authentication and a buzzer provides an additional layer of security, making it difficult for unauthorized individuals to bypass the system.

Designed for modern homes, offices, and high-security areas, this Smart Door Lock System offers a cost-effective, scalable, and reliable solution to traditional security challenges. By utilizing Raspberry Pi and machine learning-based face recognition[2], the project contributes to the advancement of smart security technologies, making access control systems more intelligent, user-friendly, and tamper-proof.

###### PROBLEM STATEMENT

Ensuring secure and reliable access control is a significant challenge in modern security systems. Traditional locking mechanisms such as mechanical keys, PIN-based keypads[6], and RFID cards are vulnerable to theft, duplication, and unauthorized access. Biometric-based security, particularly face recognition[2], offers a more robust alternative, but many existing implementations rely on computationally intensive deep learning models, which are not feasible for low-power embedded systems like the Raspberry Pi[1].

This project aims to develop an efficient and secure smart door lock system that leverages Histogram of Oriented Gradients (HOG)-based face recognition, ultrasonic sensing, OTP-based authentication, and a buzzer for enhanced security. The key challenges addressed in this project include:

1. **Lightweight Face Recognition** – Instead of computationally heavy CNN models, the system uses the HOG algorithm, which provides fast and accurate face detection and recognition while being optimized for resource-limited devices like Raspberry Pi[1].
2. **Unauthorized Access Prevention** – To enhance security, the system integrates an ultrasonic sensor to detect approaching individuals and trigger face recognition[2] only when necessary, preventing unnecessary processing and reducing power consumption.
3. **Multi-Layer Authentication** – In case face recognition[2] fails due to low-light conditions, facial occlusions, or variations in facial expressions, an OTP-based backup authentication is implemented. A GSM[5] module sends an OTP to a registered mobile number, which can be entered using a 4x4 matrix keypad[6].
4. **Intruder Detection and Alerts** – To prevent repeated unauthorized access attempts, the system includes a security alert mechanism. If multiple failed attempts are detected, an intruder alert SMS is sent to the registered user, notifying them of potential security threats. Additionally, a buzzer is activated to audibly alert nearby individuals of unauthorized attempts, further deterring intruders.
5. **Low Power and Cost-Effective Implementation** – The entire system is designed using cost-effective components, ensuring affordability without compromising security. The use of Raspberry Pi[1], a solenoid lock, and minimal hardware makes it a practical solution for residential and commercial applications.

This project effectively addresses the limitations of traditional locks and deep learning-based face recognition[2] systems by providing a lightweight, multi-layered security solution that ensures both convenience and safety. By integrating biometric authentication, OTP verification, and real-time security alerts with a buzzer, the system offers a robust and reliable smart access control mechanism suitable for modern security needs.

###### METHODOLOGY

The smart door lock system is designed using a multi-layered authentication mechanism that integrates face recognition[2], ultrasonic sensing, OTP-based verification, and a buzzer alert system to ensure enhanced security. The methodology followed in this project consists of six key phases:

**1. Hardware Setup and Configuration**

The system is built using a Raspberry Pi[1], connected to various hardware components:

* **Pi Camera** – Captures real-time images for face recognition.
* **Ultrasonic Sensor** – Detects approaching individuals and triggers face recognition only when an object is within a specified range (e.g., 50 cm).
* **Solenoid Lock** – Controls door locking/unlocking based on authentication results.
* **LED Indicators** – Provides feedback on authentication status (**Green:** Access Granted, **Red:** Access Denied).
* **4x4 Keypad** – Allows manual entry of OTP if face recognition fails.
* **GSM Module** – Sends OTP and security alerts via SMS.
* **Buzzer** – Sounds an alarm when multiple incorrect OTP attempts are made, alerting nearby individuals to unauthorized access.

**2. Face Recognition Training**

To recognize authorized users, the system trains a face recognition model using the Histogram of Oriented Gradients (HOG) algorithm. The process involves:

1. Capturing multiple images of each authorized person.
2. Extracting face encodings using HOG and storing them in a pickle file for later use.
3. Serializing the encodings to enable real-time face recognition.  
   This method ensures the system can efficiently recognize faces without requiring computationally expensive deep learning models.

**3. Real-Time Face Recognition**

When an individual approaches the door:

1. The ultrasonic sensor detects motion and activates the Pi Camera to capture an image.
2. The captured image is processed, and facial features are extracted and compared with stored face encodings using Euclidean distance matching.
3. If a match is found, the solenoid lock is triggered to unlock the door, and an SMS notification is sent to the owner confirming access.
4. If no match is found, access is denied, an alert is triggered, and the red LED indicates an unauthorized attempt.

**4. OTP-Based Backup Authentication**

If face recognition[2] fails due to poor lighting, facial occlusions, or recognition errors, the system provides an alternative authentication method:

1. A random OTP is generated and sent via GSM[5] module to the registered mobile number.
2. The user must enter the OTP using the 4x4 keypad.
3. If the OTP matches, the door unlocks successfully.
4. If multiple incorrect OTP attempts occur:
   * A buzzer is activated, producing a loud alarm to alert nearby individuals.
   * An intruder alert SMS is sent to the owner.
   * The system enters a temporary lockdown mode to prevent further access attempts.

**5. Security Measures and Alerts**

To further enhance security, the system incorporates additional protective features:

* **Retry Limits** – If face recognition fails multiple times, the system locks further attempts temporarily to prevent brute-force attacks.
* **Intruder Alert System** – If an intruder repeatedly tries incorrect OTPs, a security alert is sent to the owner along with buzzer activation.
* **Automatic Locking** – After a successful unlock, the door automatically locks again after a preset duration, ensuring continuous security.

**6. System Testing and Optimization**

The system undergoes rigorous testing under different conditions to ensure:

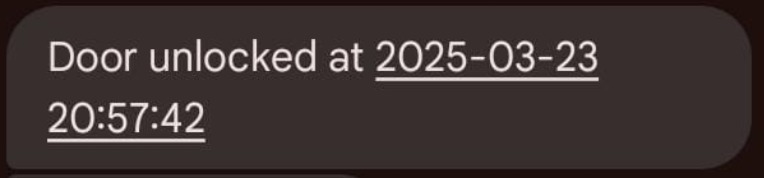
* Accuracy of face recognition under different lighting conditions and facial angles.
* Ultrasonic sensor reliability in detecting individuals within the correct distance.
* Correct functionality of OTP authentication, GSM-based alerts, and buzzer activation for intruder detection.

Through this structured methodology, the smart door lock system achieves high security, efficiency, and reliability, providing a cost-effective, real-time authentication solution for residential and commercial applications.

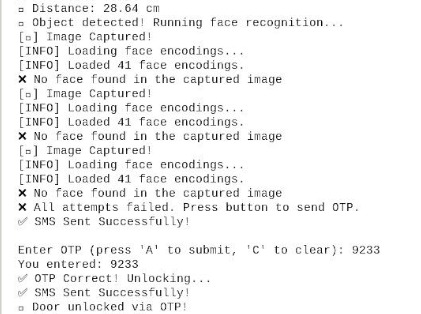
###### RESULTS

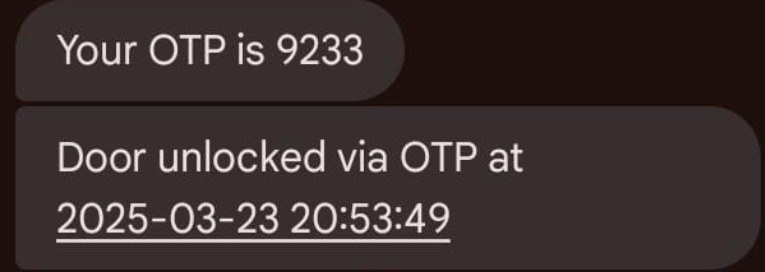
Case-1 : When the home owner is infront of the door



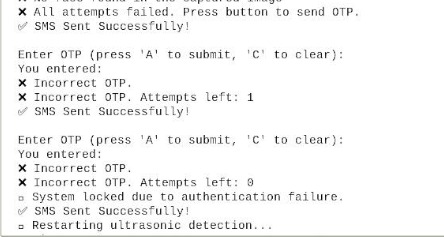


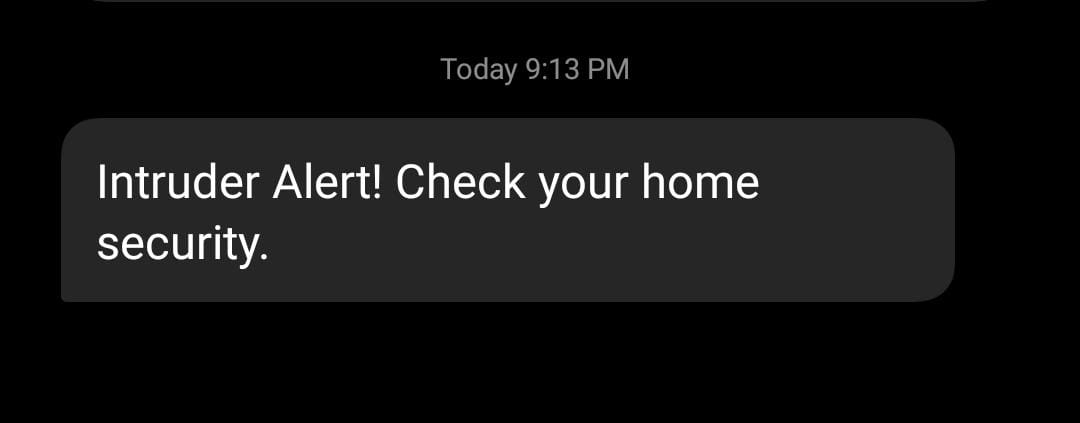
Case-2 : When the camera is not detecting, we are moving to OTP option :





Case-3 : When the thief is trying to enter, the camera and OTP gets failed and intruder alert will be sent to the owner.





**CONCLUSIONS & FUTURE WORK**

**Conclusion**

The Smart Door Lock System developed in this project integrates face recognition, ultrasonic sensing, OTP-based authentication, and a buzzer alert system to provide a highly secure and automated access control solution. By utilizing Raspberry Pi[1], Pi Camera, a solenoid lock, GSM[5] module, and a 4x4 keypad, the system ensures real-time face recognition and a secondary OTP verification mechanism. The HOG (Histogram of Oriented Gradients) algorithm allows for efficient and lightweight facial authentication, making the system ideal for resource-limited embedded devices.

The multi-layered authentication approach significantly enhances security by preventing unauthorized access while ensuring alternative authentication methods in case of face recognition failures. The integration of an ultrasonic sensor for motion detection optimizes processing efficiency, while the buzzer and intrusion alert system further strengthen security. The successful implementation and testing of this system demonstrate its practical applicability in residential, commercial, and high-security environments, offering a cost-effective, automated, and tamper-resistant security solution.

**Future Work**

To further improve the functionality, reliability, and scalability of the Smart Door Lock System, the following enhancements can be considered:

1. **Mobile Application for Remote Control & Monitoring**
   * Develop a mobile app to remotely unlock/lock the door, receive real-time access notifications, and manage user permissions.
   * Integrate biometric authentication (fingerprint or face unlock) in the mobile app for added security.
2. **Cloud-Based Access Logs & AI-Driven Security**
   * Store access attempts, face recognition logs, and OTP verification records on a secure cloud platform.
   * Implement real-time monitoring via a web dashboard for centralized security management.
   * Use machine learning-based anomaly detection to identify and alert unusual access patterns or potential security threats.
3. **Battery Backup for Power Failures**
   * Implement a rechargeable battery backup system to ensure continuous operation during power outages.
   * Optimize the system’s energy consumption by incorporating a low-power sleep mode when idle.
4. **Enhanced Face Recognition with AI & Anti-Spoofing Mechanisms**
   * Upgrade face recognition with deep learning-based models (e.g., CNNs) to improve accuracy under varying lighting conditions.
   * Implement liveness detection and anti-spoofing measures to prevent unauthorized access using printed photos or video playback.
5. **Smart Home & IoT Integration**
   * Connect the system with smart home assistants (e.g., Alexa, Google Assistant) for voice-controlled access.
   * Enable proximity-based unlocking using Bluetooth or WiFi, allowing doors to unlock automatically when an authorized user approaches.
6. **Multi-User Role-Based Access Control**
   * Implement a multi-user authentication system where different users (e.g., family members, employees, visitors) have predefined access permissions.
   * Introduce temporary access codes for guests that automatically expire after a set duration.

By incorporating these advancements, the Smart Door Lock System can evolve into a more intelligent, user-friendly, and highly secure access control solution, making it adaptable to modern security needs and future-proofing it against emerging threats.

###### REFERENCES

1. V. Bhutra, H. Kumar, S. Jangid, and L. Solanki, “Door Security using Face Detection and Raspberry Pi,” IOP Conf. Ser. Mater. Sci. Eng., vol. 331, no. 1, 2018, doi: 10.1088/1757899X/331/1/012011.
2. “IoT based facial recognition door access control home security system using raspberry pi” ,Syafeeza Ahmad Radzi, M.K. Mohd Fitri Alif, Y. Nursyifaa Athirah, A. S. Jaafar, A. H. Norihan, M. S. Saleha
3. K. Umamaheswari and P. Mahitha, "Smart security system for door access based on unique authentication," 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2021, pp. 1474-1477
4. Chakraborty, P., Sultana, S. (2022). IoT-Based Smart Home Security and Automation System. In: Sharma, D.K., Peng, SL., Sharma, R., Zaitsev, D.A. (eds) Micro-Electronics and Telecommunication Engineering . ICMETE 2021. Lecture Notes in Networks and Systems, vol 373. Springer, Singapore.
5. Soe Sandar | Saw Aung Nyein Oo "Development of a Secured Door Lock System Based on Face Recognition using Raspberry Pi and GSM Module" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-5, August 2019
6. S. Pawar, V. Kithani, S. Ahuja and S. Sahu, "Smart Home Security Using IoT and Face Recognition," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 2018, pp. 1-6
7. Vamsi, ThulluriKrishna, Kanchana Charan Sai, and M. Vijayalakshmi. "Face recognition based door unlocking system using Raspberry Pi." *International Journal of Advance Research, Ideas and Innovations in Technology* 5.2 (2019): 1320-1324.
8. Azmi, Fadhillah, Insidini Fawwaz, and Rina Anugrahwaty. "Smart door system using face recognition based on Raspberry Pi." *INFOKUM* 10.1 (2021): 360-369.