Door Lock System Using Face Recognition

Pranavi Tukaram Phavade[1], Dr. C. V. Rane[2]

[1] JSPM's, Rajarshi Shahu College of Engineering, Department of Electronics and Telecommunication Engineering. Email: pranavi.phhavade19@gmail.com
[2] Prof., JSPM's, Rajarshi Shahu College of Engineering, Department of Electronics and Telecommunication Engineering. Email: ranecharushilav@gmail.com

Abstract
There are now security issues in all zones. To circumvent these constraints, existing technology must be used. Face recognition technologies will be used in this investigation. This application collects and compares database photos to human photographs. Unauthorised entry and exit detection is an essential part of any home security system. Face recognition and other biometric identification technology can replace pins and passwords. Our goal is to create a smart door that uses our identification to safeguard the entrance.Our goal is to develop a Raspberry Pi 3-based system that only lets you into the house if your face is recognised by Harcascade algorithms. The homeowner can then remotely watch the entryway. When someone approaches the door, the system recognises their face and opens it if they are registered. If they are not registered, an alarm is sent, and a photo is taken and sent to the registered number. Here's how the system works.

Keywords: Raspberry Pi, GSM, Camera, Relay and Electric Lock, Har Cascade Algorithm.

I. Introduction

A smart door lock with facial verification is an example of a sophisticated security system that incorporates image processing, artificial intelligence (AI), and Internet of Things (IoT) connectivity. It provides a keyless, automatic, and secure alternative to access control. This technology substitutes basic locks with a more sophisticated verification mechanism, ensuring that only authorised workers access a building. It is especially useful in homes, offices, and high-security zones where standard identification techniques such as fingerprint scans, keys, and passwords may be insecure or impractical. As smart home automation and AI-powered security gained popularity, facial recognition technology emerged as a dependable and practical means of improving access management.

The system's main processing device, the Raspberry Pi, powers the smart door lock. A camera at the gate is constantly monitoring for incoming vehicles. When a person attempts to enter, the camera records their face and sends the image data to the Raspberry Pi for further processing. The system then examines the facial characteristics and compares them to previously saved images in the database, using AI-based face recognition algorithms like OpenCV, Haar cascades, and deep neural networks. When the system recognises the face of an authorised user, it opens the door.

After a relay module checks the user's identity, the Raspberry Pi instructs the electric lock to unlock and grant entry. This technique is quick and straightforward, requiring only a few seconds to complete. If the face cannot be identified, the system blocks entrance and implements additional security measures to prevent unauthorised access.If someone attempts to enter without permission or identity, the device will sound a buzzer to notify homeowners or security professionals of the impending incursion. To boost security and response time, the system employs a GSM module that sends a warning message or real-time SMS to the owner's phone following many unsuccessful attempts. This proactive defence approach assures that the property is safe even when the owner is not present.

Furthermore, cloud-based storage for access records can be included into the system. This feature enables property owners or security managers to monitor potential threats and review previous access attempts. The smart lock system is extremely adaptable because it may be used to temporarily allow visitors or delivery personnel in while limiting admittance during certain hours.This smart door lock enhances automation and convenience while also increasing security. Because this technology employs

facial recognition rather than keys, as standard locks do (for example, when carrying groceries or bags), it is especially useful for persons who have active hands. The system can be connected to smart home assistants, Internet of Things programs, and smartphone apps to allow for remote access.

II. Literature Survey

Nakandhrakumar, R. S. et al. [1] RFID, face recognition, fingerprint scanning, password authentication, and Internet of Things connectivity are all included in the proposed system to enhance security. An image recognition system matches the visitor's face to one captured by a camera sensor. The door will open once a match is found. This is comparable to how a fingerprint sensor uses a matching algorithm to confirm an identity. The RF card and password system provides extra authentication possibilities. The Raspberry Pi and Internet of Things-based connectivity utilised in the system's design allow for remote monitoring and real-time alerts via smartphone notifications, hence increasing security.

Chaitanya Kolluru et al. [2] This paper proposes a smart door lock system based on facial recognition that authenticates users via machine learning, servo motor control, and the Internet of Things. To determine identity, a Raspberry Pi-based machine learning application analyses data from camera-captured facial photos. Following proper verification, the servo motor, which also serves as an electronic lock, unlocks the door. IoT connectivity also enables real-time monitoring and remote access control, which increases user convenience and security.

M. Balaji et al. [3] To improve security, the proposed method combines OTP verification and biometric identity (facial recognition or fingerprint). When a user seeks to get access, a biometric sensor captures their fingerprint or face data, which is then analysed using pattern-matching algorithms. After successful biometric authentication, the registered user will receive an OTP via SMS. The technology provides dual-layer security with IoT-based monitoring, unlocking the door only when the right OTP is entered.

Nagasree Y Lakshmi Venkata et al. [4] The proposed system includes an ESP32-CAM with AI-Thinker for facial recognition and a solenoid lock for authentication. The ESP32-CAM supports offline face matching by recording and saving accepted faces to an SD card, which improves security. When someone stands in front of the door, the system compares their face to previously captured images. If a match is found, the solenoid lock is activated, unlocking the door; otherwise, access is denied, resulting in secure and cost-effective authentication.

Bima Sena Bayu Dewantara et al. [5] This article describes a biometric door access system that employs illumination-invariant facial recognition on an embedded device like the Raspberry Pi or Lattepanda. To improve recognition accuracy, the technique employs lighting normalisation algorithms and facial image collection. The processed photos are then compared to a previously saved database via a face matching technique. If a match is discovered, the electronic keylock is unlocked. The system is a successful security augmentation because of its low cost, ease of use, and constant performance over a wide range of lighting situations.

Khalimov R et al. [6] This paper proposes an intelligent door locking system based on facial recognition to provide secure and autonomous access control. The system recognises, extracts features from, and identifies faces with an Arduino UNO and an Android smartphone running the OpenCV library. Additionally, it uses PIN and RFID as secondary security measures. The method is effective and user-friendly since it emphasises the system's independence, low cost, and ease of database upgrades using the Android operating system.

Daniel Anando Wangean et al. [7] This paper presents a real-time facial recognition solution for smart door lock security based on the OpenCV LBPH facial recogniser and Haar Cascade. After identifying faces using Haar Cascade, the system uses OpenCV's LBPH approach to identify them in images. The system, which was built with OpenCV and Python, controls access by identifying permitted faces. The evaluation achieves 62.7% accuracy using the present dataset; more data and deep learning methods may lead to an improvement. Effective facial recognition is an essential component of any safe, automated access control strategy.

HYUNG-JIN MUN et al. [8] This study shows how to set up a guest authentication system with a webcam for facial recognition, CCTV, and a Jetson Nano. After gathering and annotating facial data with seven distinct aspects, the technique applies deep learning to identify facial characteristics. If four or more features are identified, 81 feature vectors are used to compare the face to previously recorded user data. The technology also keeps track of visitor information for security purposes. The Jetson Nano's tiny-YOLOv3 model achieves 86.3% accuracy and a detection speed of 6.5 FPS for real-time authentication.

Muhammad Waseem et al. [9] This study proposes a hierarchical network (HN) framework for facial recognition in a smart door lock system. FaceNet face embeddings confirm the system's initial face detection findings using pre-trained architectures. The system is built around the Raspberry Pi, which includes real-time facial recognition for further security. The study used a dataset of twelve University of Sindh students to demonstrate that the HN framework outperforms previous methodologies and can handle randomly selected faces from the internet. The technology depends primarily on deep machine learning techniques to detect faces rapidly and accurately.
Amritha Nag et al. [10] This article looks at a door access control system that uses facial recognition and the Internet of Things to increase security. The system supports picture capture, automated door management, email notifications, and facial recognition. The system combines OpenCV and Eigenfaces to accurately recognise faces and stores facial data from different users in a database. You may operate your door lock remotely using the Telegram app for Android. For security reasons, the captured facial photos are delivered to the authorised individual's email account. A Raspberry Pi is used to process data and communicate in real time.

III. Methodology

This door lock mechanism employs facial recognition technology to grant or deny entrance. As the visitor approaches the entryway, a camera captures their image. The system then searches the image for and recognises the face. If the system detects that the captured face matches an approved individual in its database, the electronic lock unlocks the door and enables entry. To document the attempted access, the system can record the unauthorised face and send it to designated people via email or SMS. If the face cannot be detected, a bell will sound to alert the individual.

3.1Algorithm

Harcascade Algorithm:

Haar Cascade is a machine learning-based algorithm that detects faces, eyes, and other image components. It was created by Viola and Jones and detects the difference in pixel brightness across nearby sites using rectangular patterns known as Haar-like features. These traits can be used to identify specific structures like lines, edges, and contrast zones.
To properly process and filter image areas, the system employs a number of classifiers, also known as trained decision trees. The cascade structure allows the technique to swiftly reject regions that are unlikely to contain the item, freeing up processing capability for more likely locations in the image. To accomplish accurate object recognition, the system is trained on large datasets that include both positive and negative samples. It is commonly used in facial recognition and security applications because of its real-time detection capability.

IV. Block Diagram

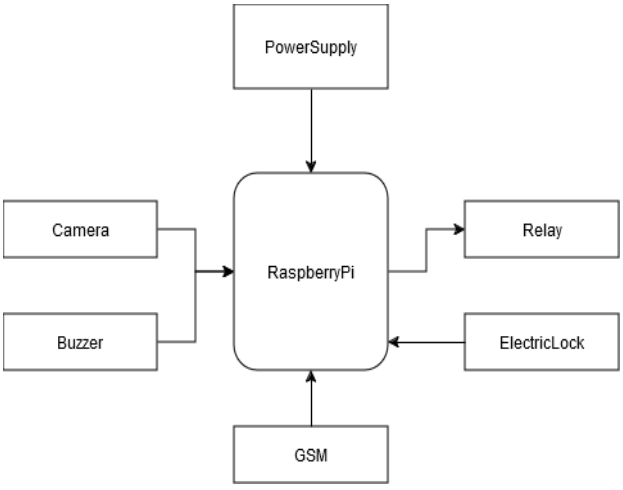

Fig 1: Block Diagram of a Face Recognition Door Lock System.

Figure 1 shows the hardware configuration of a facial recognition door lock system. A power supply unit provides electricity to all system components. The Raspberry Pi, the system's main single-board computer, controls and monitors everything. The Pi's camera allows it to photograph everyone who enters the building. The Pi employs image analysis to recognise and distinguish faces. A GSM module can be added to the Pi to allow features such as SMS notifications and remote control. The relay module connects the Pi and the electric lock. When the Pi detects a recognisable face, it triggers the relay, which unlocks the door. However, the Buzzer alerts the Pi when it detects a face it has never seen before. This system employs facial recognition technology to deliver an automated, safe, and secure access control solution.

4.1 Hardware Requirement:

Raspberry Pi:

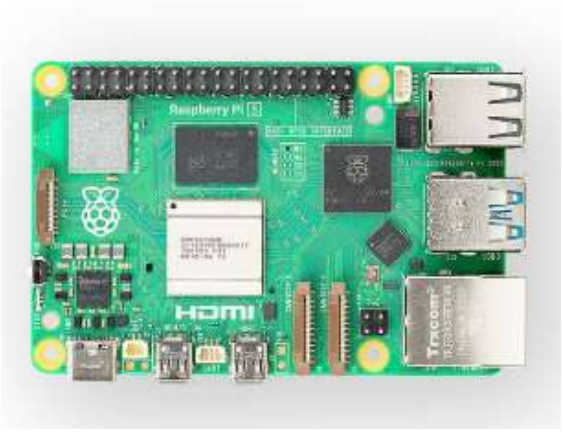

Fig: Raspberry Pi

The Raspberry Pi is perfect for usage in smart systems because of its processor, memory, USB ports, GPIO pins, and wireless connectivity. Additionally, it can be linked to sensors and other devices. Because it is compatible with Python and other computer languages, it facilitates developers' ability to generate creative ideas.A face recognition-based door unlocking system that integrates hardware control and computer vision is powered by the Raspberry Pi. Real-time images captured by the Raspberry Pi's camera module are subsequently processed by facial recognition programs like TensorFlow or OpenCV. The models are used to find the necessary faces. The GPIO pins on the Raspberry Pi activate an electronic door lock to allow entrance when a match is discovered.

Camera:

Fig: Camera

Cameras are important sensors in Internet of Things systems because they collect visual data that may be utilised for tasks including object detection, surveillance, facial recognition, and real-time monitoring. These cameras connect to Internet of Things devices to collect photos or record videos. The photographs or videos are then either reviewed locally or transferred to the cloud for analysis. Because IoT cameras are often small, networked, and low-power, they can be easily connected to microcontrollers or single-board computers like the Raspberry Pi.

Electric Lock:

Fig: Electric Lock

An electric lock is a complicated locking mechanism powered by electricity that is frequently coupled to smart devices in Internet of Things systems for added convenience and security. Unlike traditional locks, electronic locks use actuators to engage and disengage the locking mechanism. These actuators can be controlled remotely using Internet of Things devices like smartphones, tablets, and smart hubs.These locks are typically Wi-Fi, Bluetooth, or Zigbee compatible, allowing you to easily connect to a centralised control system. Electric locks come with adjustable access control features, including fingerprint recognition, password entry, and real-time monitoring.

Buzzer:

Fig: Buzzer

Buzzers, small sound-producing devices, are used by Internet of Things systems to give audio alerts or warnings. Electrical impulses are routinely turned into sound using piezoelectric or electromagnetic devices. Buzzers are small, low-power devices that can be readily linked to microcontrollers like Arduino or Raspberry Pi via GPIO connections. Buzzers are used in IoT systems to offer audio feedback on a wide range of events, such as security issues, critical alarms, system failures, and successful operations.

GSM:

Fig: GSM

GSM (Global System for Mobile Communications) is a mobile telecommunications standard that enables devices to connect to cellular networks and send and receive voice, text, and data messages. GSM, which was created in the 1990s, transmits digital signals using frequencies like 900 and 1800 MHz. In addition to being used for user authentication, SIM cards offer data services like SMS and GPRS. Devices like trackers, smart meters, and remote monitoring systems may now communicate with each other across mobile networks thanks to the extensive use of GSM in Internet of Things applications.

V. Flowchart

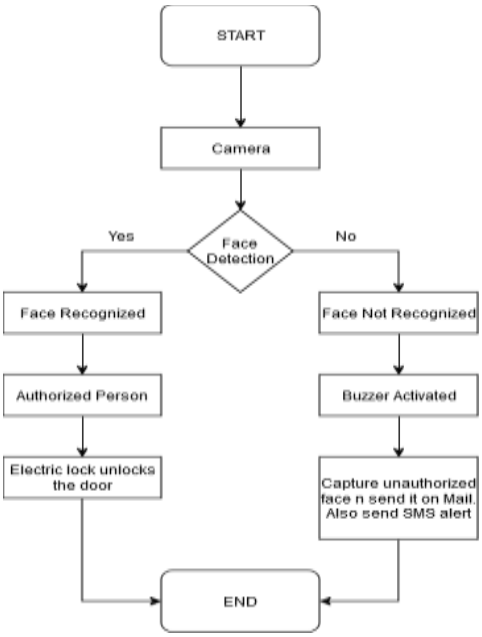

Fig 2: Flowchart

Figure 2 illustrates The facial recognition smart door lock system is a sophisticated security feature that regulates building access. To begin the process, a camera snaps a picture of the person at the door. The device then detects faces by comparing the captured photographs to a database of previously registered and approved users. If the system detects the person's face and determines that they are acceptable, the electronic lock unlocks the door and lets them in. This simple, automated solution enhances convenience and security by removing the need for traditional keys and access cards.

However, if the user's face is not recognised, the system considers them unapproved. In some cases, an alert is issued to advise surrounding personnel of a potential intrusion. The device takes a snapshot of the unauthorised person and transmits it to the homeowner or security authority via email for verification. An SMS alert is also intended to promptly notify clients of any unauthorised access attempts.

Our innovative security solution effectively blocks unauthorised access while offering a seamless experience for authorised users. By combining facial recognition, automated alarms, and remote monitoring, it enhances security, reduces risks, and delivers a more efficient access management solution for homes, workplaces, and other critical areas.

VI. Result

The face recognition-based door lock system was successfully implemented using the Raspberry Pi 4 Model B. The system utilized the OpenCV library for face detection and recognition, integrating the Haar Cascade classifier for detection and the LBPH (Local Binary Pattern Histogram) algorithm for recognition. The following outcomes were observed during testing:

Face Detection Accuracy: The system accurately detected faces under good lighting conditions and a clear frontal view. On average, detection occurred in under 2 seconds.

Recognition Accuracy: The LBPH algorithm achieved a recognition accuracy of 92% for known faces when trained on 20 images per person. Recognition failed occasionally due to:

Low lighting
Partial occlusions (e.g., wearing a mask or cap)

Drastic changes in appearance (e.g., beard growth)

System Response Time: From the moment a face was detected to the door unlocking, the response time ranged between 3 to 5 seconds.

User Interface: The LCD displayed real-time feedback such as "Face Detected", "Access Granted", or "Access Denied". Unknown users were prompted with a message and denied access.

Security Functionality: The door lock remained in a locked state for unrecognized faces and did not respond unless the face matched the stored data and also shares a text on registered phone number and the image of unrecognized person over a Email .

VII. Discussion

The implemented system demonstrates that Raspberry Pi is capable of handling real-time face recognition tasks efficiently for low-security applications such as home or office automation. The LBPH algorithm proved to be a good choice due to its simplicity and effectiveness in recognizing faces with moderate variations in appearance.
However, there were several limitations:

- **Lighting Sensitivity:** Performance degraded in low light or against highly lit backgrounds. This suggests the potential benefit of integrating an infrared camera or better ambient light control.
- **Scalability:** As the number of registered users increases, the processing time for recognition also increases slightly. For large-scale applications, a more powerful processor or offloading recognition to cloud services could be considered.
- **Security Considerations:** While face recognition adds a layer of convenience, it can be spoofed with photos or videos in the absence of liveness detection. Future work could integrate an anti-spoofing module using motion, blink detection, or 3D sensors.
- **Data Storage and Management:** The system stores images locally on the Raspberry Pi, which can be a concern for data privacy and long-term usage. Implementing secure cloud storage or encryption can improve this aspect.

VIII. Conclusion

This project shows how to use a Raspberry Pi and a GSM module to build a secure face recognition-based door lock system. Our system provides users with energy efficiency, comfort, convenience, and security locks.This setup includes a Raspberry Pi, webcam, relay, GSM module, and a solenoid door lock.The Raspberry Pi design is superior to a computer-based facial recognition system since it is lighter, more portable, and more adaptable. Also, explain the significance of the security warning to the chosen individual.In the event of a power outage, we provide power backup to keep the system operating. The Raspberry Pi is charged using a power bank to reduce the possibility of it slowing down.Finally, a reliable IoT and facial recognition security solution was created. When an unexpected person is spotted via the Internet of Things, customers can be identified and notified using face recognition technology.
Artificial intelligence and machine learning enable facial recognition systems to handle changes such as masks and accessories while also operating better in a variety of lighting conditions. Multi-factor authentication improves security by integrating fingerprint or voice verification with facial recognition. While reducing reliance on cloud computing, edge processing and real-time data encryption can boost operational speed and security.

References

1. Venkatasamy, Ramkumar, Joshuva Arockia Dhanraj, S. Aravinth, and K. Balachandar. "Design and Development of IOT based Smart Door Lock System." In 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT), pp. 1525-1528. IEEE, 2022.

2. Kolluru, Chaitanya, G. V. Akhil, Krishna Reddy, and Aruru Sai Kumar. "Development of Face Recognition-Based Smart Door Lock System with Remote Servo Control Authentication." In 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1-6. IEEE, 2023.
3. Balaji, M., N. Padmaja, Nelaturu Swathi, Shaik Atheek, Midabalam Manasa, and Katheragandla Charan Kumar. "Biometric-based Smart Door Locking System using Biometric and OTP." In 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pp. 898-903. IEEE, 2023.
4. Venkata, Nagasree Y. Lakshmi, Ch Rupa, B. Dharmika, Teja G. Nithin, and N. Vineela. "Intelligent secure smart locking system using face biometrics." In 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), pp. 268-273. IEEE, 2021.
5. Dewantara, Bima Sena Bayu, Mochamad Mobed Bachtiar, and Syah Embo Lantang. "Door Access Control based on Illumination Invariant Face Recognition in Embedded System." In 2020 10th Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS), pp. 105-110. IEEE, 2020.
6. Khalimov, R., Z. Rakhimbayeva, A. Shokayev, B. Kamalov, and Md Hazrat Ali. "Development of intelligent door locking system based on face recognition technology." In 2020 11th International Conference on Mechanical and Aerospace Engineering (ICMAE), pp. 244-248. IEEE, 2020.
7. Wangean, Daniel Anando, Sinjiru Setyawan, Fairuz Iqbal Maulana, Gusti Pangestu, and Choirul Huda. "Development of Real-Time Face Recognition for Smart Door Lock Security System using Haar Cascade and OpenCV LBPH Face Recognizer." In 2023 International Conference on Computer Science, Information Technology and Engineering (ICCoSITE), pp. 506-510. IEEE, 2023.
8. Mun, Hyung-Jin, and Min-Hye Lee. "Design for visitor authentication based on face recognition technology Using CCTV." IEEE Access 10 (2022): 124604-124618.
9. Waseem, Muhammad, Sundar Ali Khowaja, Ramesh Kumar Ayyasamy, and Farhan Bashir. "Face recognition for smart door lock system using hierarchical network." In 2020 International Conference on Computational Intelligence (ICCI), pp. 51-56. IEEE, 2020.
10. Nag, Amritha, J. N. Nikhilendra, and Mrutyunjay Kalmath. "IOT based door access control using face recognition." In 2018 3rd International conference for convergence in technology (I2CT), pp. 1-3. IEEE, 2018.
11. Yedulapuram, Sharvani, Rajeshwarrao Arabelli, Kommabatla Mahender, and Chintoju Sidhardha. "Automatic door lock system by face recognition." In IOP Conference Series: Materials Science and Engineering, vol. 981, no. 3, p. 032036. IOP Publishing, 2020.
12. Hassan, Harnani, Raudah Abu Bakar, and Ahmad Thaqib Fawwaz Mokhtar. "Face recognition based on auto-switching magnetic door lock system using microcontroller." In 2012 International conference on system engineering and technology (ICSET), pp. 1-6. IEEE, 2012.
13. Roy, Sourav, Md Nasir Uddin, Md Zahirul Haque, and Md Jahidul Kabir. "Design and implementation of the smart door lock system with face recognition method using the Linux platform Raspberry Pi." by IJCSN-International Journal of Computer Science and Network 7, no. 6 (2018).
14. Waseem, Muhammad, Sundar Ali Khowaja, Ramesh Kumar Ayyasamy, and Farhan Bashir. "Face recognition for smart door lock system using hierarchical network." In 2020 International Conference on Computational Intelligence (ICCI), pp. 51-56. IEEE, 2020.
15. Sandar, Soe, and Saw Aung Nyein Oo. "Development of a secured door lock system based on face recognition using Raspberry Pi and GSM module." Development 3, no. 5 (2019).
16. Lwin, Hteik Htar, Aung Soe Khaing, and Hla Myo Tun. "Automatic door access system using face recognition." international Journal of scientific & technology research 4, no. 6 (2015): 294-299.
17. Zhu, Zhiguo, and Yao Cheng. "Application of attitude tracking algorithm for face recognition based on OpenCV in the intelligent door lock." Computer Communications 154 (2020): 390-397.
18. Lim, Jimin, Chan Kim, Wonsuk Cha, Taemoon Han, Guewon Huh, Sanggeun Song, and Sangjun Lee. "Reliable digital door lock control system using face recognition." Journal of IKEEE 17, no. 4 (2013): 499-504.
19. Saputra, Rezki, and Nico Surantha. "Smart and real-time door lock system for an elderly user based on face recognition." Bulletin of Electrical Engineering and Informatics 10, no. 3 (2021): 1345-1355.
20. Phawinee, Suphawimon, Jing-Fang Cai, Zhe-Yu Guo, Hao-Ze Zheng, and Guan-Chen Chen. "Face recognition in an intelligent door lock with ResNet model based on deep learning." Journal of Intelligent & Fuzzy Systems 40, no. 4 (2021): 8021-8031.