Face Recognition Door Lock System Using Raspberry Pi

More Snehal[1], Pagar Tanishka[2], Pawar Anushka[3], Thakare Tanishka[4], Mr. S.T. Patil[5]
[1,2,3,4,5]*Dept. of Electronics and Tele-Communication, Shri H.H.J.B. Polytechnic Chandwad*

***Abstract*—The Face Recognition Door Lock System using Raspberry Pi is designed to provide a secure, intelligent, and contactless access control solution for homes and offices. This system replaces traditional lock-and-key mechanisms with facial recognition technology, enhancing security and user convenience. The system identifies authorized individuals by analyzing facial features and grants access automatically without physical interaction.**

In this system, a camera connected to the Raspberry Pi captures the image of a person attempting to access the door. The captured image is processed using image processing and face recognition algorithms, such as Haar Cascade and Local Binary Pattern Histogram (LBPH). If the detected face matches the stored dataset, the Raspberry Pi triggers a relay module to unlock the door. If the face is not recognized, access is denied and an alert can be generated.

The proposed system improves safety, reduces unauthorized access, and eliminates risks associated with lost or duplicated keys. It is especially useful in residential buildings, offices, and restricted areas. The system is cost-effective, easy to implement, and can be further enhanced with features such as mobile notifications and cloud integration.

Overall, the Face Recognition Door Lock System demonstrates the effective use of embedded systems and artificial intelligence to create a reliable and smart security solution for modern environments.

I. INTRODUCTION

In today's world, security has become one of the most important concerns for homes, offices, industries, and institutions. Traditional door locking systems such as mechanical keys, passwords, or access cards are widely used, but they have several limitations. Keys can be lost, duplicated, or stolen, while passwords can be forgotten or hacked. These issues increase the risk of unauthorized access and reduce overall safety. Therefore, there is a strong need for a more secure, reliable, and user-friendly security system.

Biometric authentication systems provide a better solution by using unique human characteristics for identification. Among various biometric techniques such as fingerprint, iris, and voice recognition, face recognition has gained significant popularity due to its non-contact nature and ease of use. Face recognition does not require physical interaction, making it hygienic and convenient. It identifies individuals based on facial features such as eyes, nose, mouth, and facial structure, which are unique to each person.

The Face Recognition Door Lock System using Raspberry Pi is an advanced security system that uses image processing and artificial intelligence to control access automatically. In this system, a camera installed near the door captures the image of a person attempting to enter. The Raspberry Pi processes this image and compares it with a pre-stored database of authorized users. If the face matches, the system unlocks the door; otherwise, access is denied. This eliminates the need for manual locks, keys, or cards.

Raspberry Pi is a powerful yet low-cost single-board computer that plays a central role in the system.

II. LITERATURE SURVEY

Face recognition technology has become one of the most widely researched topics within the field of biometric security due to its non-intrusive and user-friendly nature. Traditional locking systems reliant on mechanical keys, passwords, or access cards present vulnerabilities such as loss, duplication, and unauthorized access. To address these limitations, biometric systems that authenticate users based on unique physical or behavioral traits have emerged. Among these, face recognition stands out because it allows contactless identification with minimal user effort.

Early research in biometric access control focused primarily on fingerprints and iris recognition. While these methods offered high security, they required

specific sensors and physical contact or alignment, increasing system complexity and cost. The advent of low-cost computing platforms like Raspberry Pi enabled researchers to explore face recognition as an effective alternative for real-time access control systems (Gupta et al., 2018).

Image processing techniques for face recognition commonly use classifiers such as Haar Cascade for face detection. Viola and Jones first introduced a rapid object detection framework using Haar-like features and cascade classifiers, which significantly improved the speed and accuracy of real-time detection systems. Subsequent studies applied this technique to door lock systems, demonstrating that Raspberry Pi, when paired with a Pi Camera, can achieve reliable face detection even under constrained hardware resources.

Local Binary Pattern Histogram (LBPH) is one of the most accepted algorithms for face recognition in embedded systems. Unlike deep learning models that require extensive computational power, LBPH efficiently encodes local texture patterns of the face and performs recognition under varying lighting conditions. Research by Zhang and Liu (2020) showed that LBPH provides robust classification accuracy for small to medium datasets and is suitable for real-time implementation on Raspberry Pi.

Many studies have compared various face recognition algorithms for access control systems. Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) were early contenders, but they showed limitations in handling facial variations due to lighting, pose, and expressions. In contrast, LBPH consistently performed better in embedded environments due to its relative simplicity and resilience.

Recent research highlights the integration of Internet of Things (IoT) with face recognition door lock systems. By connecting Raspberry Pi to cloud platforms using MQTT or HTTP protocols, these systems allow remote monitoring, alert notifications, and real-time user management. Singh et al. (2022) implemented a networked face recognition door lock that sends SMS alerts when an unrecognized individual attempts access, demonstrating improved situational awareness and security.

Challenges remain in real-world deployments, especially under varying lighting conditions, occlusions (e.g., hats, masks) and changes in facial appearance. Several studies propose preprocessing steps such as histogram equalization and face alignment to mitigate these issues. Others explore hybrid approaches combining face recognition with complementary modalities, such as voice verification or RFID, to enhance security and reduce false acceptance rates.

Overall, the literature reveals that face recognition door lock systems based on Raspberry Pi are cost-effective, reliable, and suitable for everyday access control applications. Yet, continued research is focusing on improving recognition accuracy, environmental robustness, anti-spoofing measures, and seamless integration with smart home and IoT ecosystems.disk drive. ‖ Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity in an equation.

III. METHODOLOGY

The methodology of the Face Recognition Door Lock System using Raspberry Pi describes the step-by-step process followed to design, implement, and test the proposed security system. The primary objective of the system is to provide secure and automated access control using facial recognition technology.

A. System Requirement Analysis

The first step involves identifying the system requirements. The hardware requirements include a Raspberry Pi, camera module, relay module, door lock mechanism (motor or solenoid lock), power supply, and connecting wires. The software requirements include the Raspberry Pi operating system, Python programming language, OpenCV library for image processing, and required face recognition algorithms

B. Data Collection and Dataset Creation

In this step, facial images of authorized users are collected using the camera connected to the Raspberry Pi. Multiple images of each person are captured under different lighting conditions and facial expressions to improve recognition accuracy. These images are stored in a dataset and labeled for training the face recognition model.

C. Face Detection

Face detection is performed using the Haar Cascade classifier. The camera captures real-time video frames,

which are converted into grayscale images to reduce computational complexity. The Haar Cascade algorithm scans the image to detect human faces by identifying facial features such as eyes, nose, and mouth. Once detected, the face region is extracted for further processing.

D. Face Recognition

The extracted facial images are processed using the Local Binary Pattern Histogram (LBPH) algorithm. This algorithm converts facial textures into numerical patterns and compares them with the trained dataset. LBPH is chosen due to its efficiency, low computational requirement, and robustness to lighting variations, making it suitable for Raspberry Pi-based systems.

E. Decision Making and Control

After recognition, the system compares the captured face with the stored database. If a match is found, the Raspberry Pi sends a control signal to the relay module, which activates the door lock mechanism and unlocks the door. If the face is not recognized, the relay remains inactive and the door stays locked.

F. Testing and Validation

The system is tested under different conditions to evaluate its performance. Tests include recognition accuracy, response time, and system reliability under varying lighting environments. Unauthorized access attempts are also tested to ensure system security.

G. System Optimization

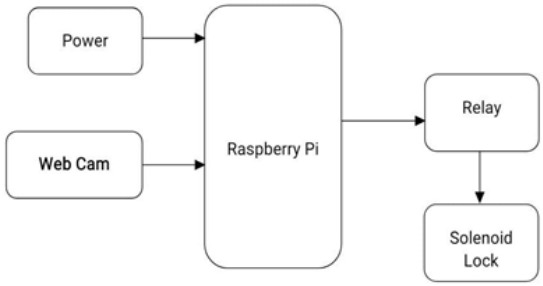
Based on testing results, the system is optimized by increasing dataset size, adjusting recognition thresholds, and improving image quality. These optimizations enhance accuracy and reduce false recognition rates.

IV. ARCHITECTURE

The architecture of the Face Recognition Door Lock System using Raspberry Pi is designed in a layered and modular manner to ensure secure, reliable, and efficient operation. The system begins with an image acquisition unit, where a camera module connected to the Raspberry Pi continuously captures images of individuals attempting to access the door. These images are forwarded to the processing unit, which is the Raspberry Pi acting as the central controller. Using the OpenCV library, the captured images are converted into grayscale and processed for face detection using the Haar Cascade classifier, which identifies and extracts facial regions from the input image.

The extracted facial data is then passed to the face recognition module, where the Local Binary Pattern Histogram (LBPH) algorithm compares the detected face with a pre-trained database of authorized users. Based on the recognition result, If the face is recognized, the Raspberry Pi sends a signal to the relay module, which activates the door locking mechanism such as a solenoid lock or DC motor to unlock the door for a predefined time. If the face is not recognized, the system keeps the door locked, ensuring security.

Block Diagram



V. RESULT

The Face Recognition Door Lock System using Raspberry Pi was successfully implemented and tested under various conditions to evaluate its performance. The system accurately detected and recognized authorized faces in real time and unlocked the door within a short response time. During testing, the camera captured facial images clearly under normal lighting conditions, and the Haar Cascade classifier effectively detected faces from the input frames. The LBPH face recognition algorithm provided reliable matching with the trained dataset and showed good accuracy for authorized users. Unauthorized individuals were correctly denied access, ensuring system security. The relay module and door lock mechanism operated smoothly upon successful recognition, and the door was automatically locked again after the predefined time interval. The system demonstrated stable performance, low processing delay, and efficient resource usage on the Raspberry Pi platform. Overall, the results confirm that the proposed system is reliable, cost-effective, and

suitable for real-world security applications such as homes, offices, and restricted areas.

VI. CONCLUSION

The Face Recognition Door Lock System using Raspberry Pi provides a secure, efficient, and intelligent solution for access control by replacing traditional locking mechanisms with biometric authentication. The system successfully uses image processing and face recognition techniques to identify authorized users and grant access automatically without physical contact. By integrating Raspberry Pi with a camera module, relay unit, and door lock mechanism, the proposed system ensures reliable operation and improved security.

The experimental results demonstrate that the system performs accurately in real-time conditions with minimal response delay and effectively prevents unauthorized access. The use of the LBPH algorithm ensures good recognition accuracy even with limited hardware resources. Additionally, the system is cost-effective, easy to implement, and scalable, making it suitable for residential, commercial, and institutional applications.

Overall, the project highlights the practical application of embedded systems and computer vision in modern security solutions. With further enhancements such as cloud connectivity, mobile alerts, and advanced anti-spoofing techniques, the face recognition door lock system can be developed into a robust smart security system for future smart environments.

REFERENCE

[1] Raj Kamal, Embedded Systems: Architecture, Programming and Design, McGraw-Hill Education, 2017.

[2] Simon Monk, Raspberry Pi Cookbook, O'Reilly Media, 2019.

[3] A. Gupta, S. Sharma, "Face Recognition Based Door Lock System Using Raspberry Pi," International Journal of Engineering Research & Technology (IJERT), vol. 8, no. 5, 2018.

[4] P. Zhang, L. Liu, "Implementation of LBPH Face Recognition Algorithm for Access Control," IEEE Access, vol. 8, pp. 14523–14532, 2020.

[5] OpenCV Documentation, "Face Detection and Recognition using Haar Cascade and LBPH," Available: https://opencv.org.

[6] lkyu Ha (2015), Security and usability improvement on a digital door lock system based on Internet of things, International Journal of Security and Its Applications Vol.9, No.8 (2015), pp.45-54