Real Time Face Recognition Security System

Maheswaran T[1], Dinesh M[2], Guhan S[3], Kamalakar L[4], Mohammed Abdulla M[5]

[1] *Professor, Electronics and Communication Engineering, Sri Shakthi Institute of Engineering and Technology, India*
E-mail: maheswaran@siet.ac.in
[2] *Electronics and Communication Engineering, Sri Shakthi Institute of Engineering and Technology, India*
E-mail: dineshm21ece@srishakthi.ac.in
[3] *Electronics and Communication Engineering, Sri Shakthi Institute of Engineering and Technology, India*
E-mail: guhans21ece@srishakthi.ac.in
[4] *Electronics and Communication Engineering, Sri Shakthi Institute of Engineering and Technology, India*
E-mail: kamalakarl21ece@srishakthi.ac.in
[5] *Electronics and Communication Engineering, Sri Shakthi Institute of Engineering and Technology, India*
E-mail: mohammedabdullam21ece@srishakthi.ac.in

ABSTRACT

This project develops a face recognition-based door unlocking system with a backup keypad for added security. It uses a Raspberry Pi 3B+ to process real-time facial recognition for primary authentication. If face recognition fails, users can enter a pre-set password on the keypad as a secondary authentication method. A stepper motor controls the locking mechanism for door access. The system enhances security by combining biometric authentication with a dual-layer approach. It provides a secure, contactless, and user-friendly access solution. The project addresses the vulnerabilities of traditional locking mechanisms like key duplication and combination lock guessing. It aims to improve both security and usability in environments where access control is critical. The system is designed to be reliable and practical for everyday use. This approach offers a modern solution to traditional door security challenges.

Keywords: Raspberry Pi, Biometric authentication, Face recognition.

1. INTRODUCTION

Traditional door locks, such as physical keys and combination locks, are vulnerable to loss, theft, and security risks. This project introduces a face recognition-based door unlocking system with a backup keypad mechanism. The primary authentication relies on facial biometrics for secure, contactless access, while the secondary keypad ensures access in case of failure. Built on a Raspberry Pi 3B+, the system utilizes real-time image processing and custom-trained facial recognition models. A stepper motor-driven locking mechanism enables smooth operation. By combining biometric authentication with a backup method, the system offers enhanced security and convenience. It is designed to provide a reliable, user-friendly solution for modern access control

2. LITERATURE SURVEY

Paper 1 - "Implementation of Human Face Detection System for Door Security using Raspberry Pi" 1. Shrutika V. Deshmukh, 2. Prof Dr. U.A. Kshirsagar, IJIREEICE, ISO 3297:2007 Certified, Vol. 5, Issue 4, April 2017.

Paper 2 - "Face Recognition Using Haar - Cascade Classifier for Criminal Identification" 1. Senthamizh Selvi R, 2. D. Sivakumar, 3. Sandhya J. S, 4. Siva Sowmiya S, Ramya S, Kanaga Suba Raja S International Journal of Recent Technology and Engineering.

Paper 3 - "Survey on real-time facial expression recognition techniques" 1. Shubhada Deshmukh, 2. Manasi Patwardhan, 3. Anjali Mahajan 1. PIET, VIT, Pune, India 2. Computer Engineering, VIT, Pune, India 3. PIET, Nagpur, India, ISSN 2047-4938.

3. METHODOLOGY

This methodology details the creation of a face recognition-based door unlocking system with a backup keypad. It involves setting up the Raspberry Pi, training the recognition model with authorized faces, and integrating the keypad for PIN input. The system uses real-time facial recognition to unlock the door and the stepper motor for locking. If recognition fails, the keypad serves as a backup. Error handling, logging, and testing ensure reliable performance before deployment.

3.1. FACE DETECTION:

For your **face recognition-based door unlocking system**, **face detection** is a crucial component for identifying authorized users. The system utilizes real-time image processing to detect faces and grant access. Using a camera connected to a Raspberry Pi 3B+, the face detection algorithm locates faces within the frame and compares them with stored data. If a face is detected, the system proceeds to facial recognition for authentication. Key challenges in face detection include dealing with varying lighting conditions, face angles, and occlusions (like masks). To ensure reliability, the system can incorporate image enhancement techniques and optimize detection algorithms for accuracy and speed

Image Quality: Poor lighting, low resolution, or camera malfunctions can hinder the detection process and affect recognition accuracy. To ensure reliable performance, it's important to use high-resolution cameras and implement techniques like automatic lighting adjustments or image enhancement to improve clarity and detail.

Observations: In face detection involve analyzing factors like lighting conditions, face angles, and any obstructions (e.g., glasses or masks) that could affect detection accuracy.

Information Alert: The system sends real-time maintenance alerts and fault predictions via email, notifying users of potential issues based on the analysis of vehicle data.

3.2. TOOLS AND TECHNOLOGIES USED

This section outlines the hardware and software tools employed in the project.

1. **Raspberry Pi 3B+**: The main processing unit that controls the system's hardware and runs the software for facial recognition, keypad input, and motor control.
2. **Python:** The programming language used for system development, including image processing, facial recognition, and integrating all components.
3. **OpenCV:** A computer vision library that enables real-time image processing and face detection in video frames from the camera.
4. **Face-recognition:** A Python library used to perform facial recognition, enabling the system to identify authorized individuals based on facial features.
5. **RPi. GPIO**: A Python library that allows the Raspberry Pi to interface with hardware components like the stepper motor and 4x4 matrix keypad through the GPIO pins.

4. IMPLEMENTATION

The system uses a Raspberry Pi 3B+ with Python for facial recognition via **face-recognition** and **OpenCV**. Authorized faces are captured, encoded, and stored for identification. **RPi. GPIO** controls the 4x4 keypad for PIN input and the stepper motor for door locking. Access is granted through either face recognition or the correct PIN, with error handling for failure.

4.1. System Design Overview

The system design includes a Raspberry Pi 3B+ that integrates a USB camera for facial recognition, a 4x4 matrix keypad for backup PIN entry, and a stepper motor to control the door lock. Facial recognition is handled using the **face-recognition** and **OpenCV** libraries to match captured faces with stored data.

If recognition fails, the user can enter a PIN for secondary authentication. The **RPi. GPIO** library controls the stepper motor to lock or unlock the door upon successful authentication. Additionally, the system incorporates error handling and logs access attempts for security purposes.

4.2. Step-by-Step Implementation Process

A. **Hardware Components:** The system consists of a Raspberry Pi 3B+, a USB camera for facial recognition, a 4x4 matrix keypad for backup PIN input, and a stepper motor for controlling the door lock**.**
B. **Facial Recognition:** The face-recognition and OpenCV libraries are used to capture and process facial images in real-time, comparing them with stored data to grant or deny access.
C. **Authentication Process:** The system first attempts facial recognition. If unsuccessful, the user can enter a PIN on the keypad as a secondary authentication method.
D. **Motor Control:** Once authenticated, the RPi. GPIO library controls the stepper motor to unlock or lock the door based on the successful authentication**.**
E. **Error Handling and Logging:** The system includes error handling for failed authentication attempts and logs access attempts for security auditing**.**

4.3. Software and Hardware Tools Used

- **Software**: **e:** Python (for system implementation and data processing), Machine Learning algorithms.
- **Hardware**: Raspberry Pi 3Bi, USB Camera, 4x4 Matrix Keypad, Stepper Motor.

4.4. System Architecture

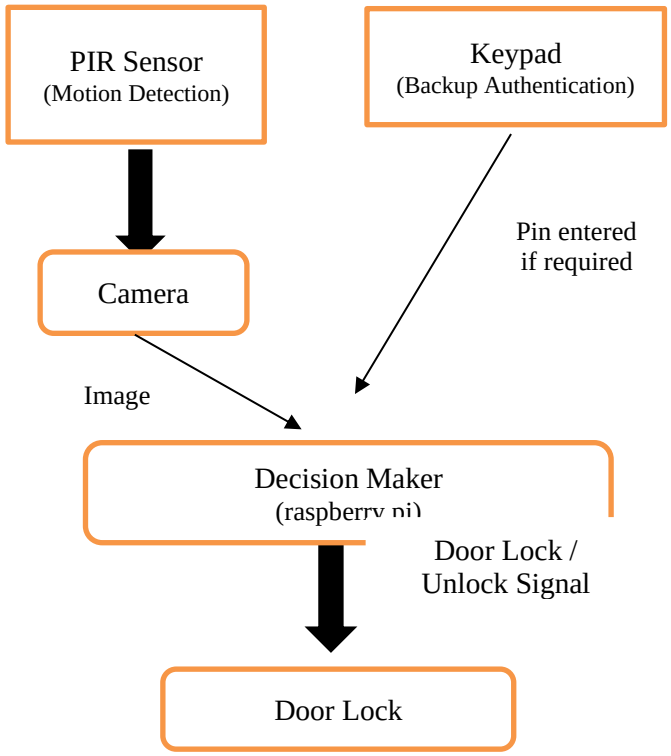

Fig. System Architecture

5.RESULTS AND DISCUSSION

5.1. Key Findings

Key findings of the project include the successful integration of facial recognition for secure, contactless access control, with a reliable backup authentication method via a keypad. The system demonstrated effective real-time image processing and accurate face matching, though challenges with lighting and angles were noted. The stepper motor functioned well for door control, and error handling ensured fallback options in case of authentication failure. Overall, the system improved security while maintaining user-friendly access.

5.2. Performance Analysis

The performance of the face recognition-based door unlocking system was generally efficient in terms of both facial recognition and access control. Facial recognition performed well under ideal conditions, with accurate matching of authorized faces. However, performance was slightly impacted by poor lighting or unusual angles, leading to occasional mismatches or failures. The system's backup PIN method via the keypad provided a reliable secondary authentication option in such cases. The stepper motor worked effectively in unlocking and locking the door, with precise control through the Raspberry Pi. Overall, the system demonstrated good functionality, though improvements in lighting conditions and recognition algorithms could enhance reliability and speed.

6.LIMITATIONS AND CHALLENGES

The main limitations of the project include potential inaccuracies in facial recognition under poor lighting or varied angles, leading to failed identification. The system's reliance on hardware components like the camera and stepper motor may cause malfunctions due to connectivity issues. Additionally, the keypad authentication can be vulnerable to PIN theft. Power outages or resource limitations on the Raspberry Pi could also affect system reliability and performance.

7. FUTURE SCOPE AND CONCLUSION

In conclusion, this project successfully developed a face recognition-based door unlocking system that combines biometric authentication with a backup PIN method, providing a secure, user-friendly alternative to traditional locks. Built on a Raspberry Pi, the system utilizes real-time facial recognition, stepper motor control for locking, and a 4x4 matrix keypad for secondary access.

It offers reliable security with error handling, logging, and audit capabilities. For future improvements, the system could integrate advanced machine learning models for enhanced facial recognition accuracy, multi-factor authentication methods, and real-time monitoring with automated alerts. Expanding to cloud-based remote access and optimizing system performance for faster recognition would further enhance usability. Additionally, making the system more power-efficient and portable could broaden its applications, making it suitable for a wider range of environments, from homes to high-security facilities. Furthermore, incorporating artificial intelligence for anomaly detection, adding a facial recognition system capable of recognizing multiple users simultaneously, and improving the system's scalability to handle large datasets could further elevate its capabilities. Integration with home automation systems, as well as features like touchless entry and motion detection, could also improve user experience and security.

8.REFERENCE

- Multi-faces recognition process using Haar cascades and eigenface method T Mantoro, MA Ayu 2018
- "Home locking system through face recognition using Raspberry Pi and GSM module" 1. Ms. Poojitha S, 2. Ms. Yashodha S.A, 3.
- Ms. Priyadarshini S, Bangalore institute of technology, Bengaluru, India, Project reference no.: 40s_be_0592
- https://research.vit.ac.in/publication/facial-recognition
  enabled-smart-door-unlock