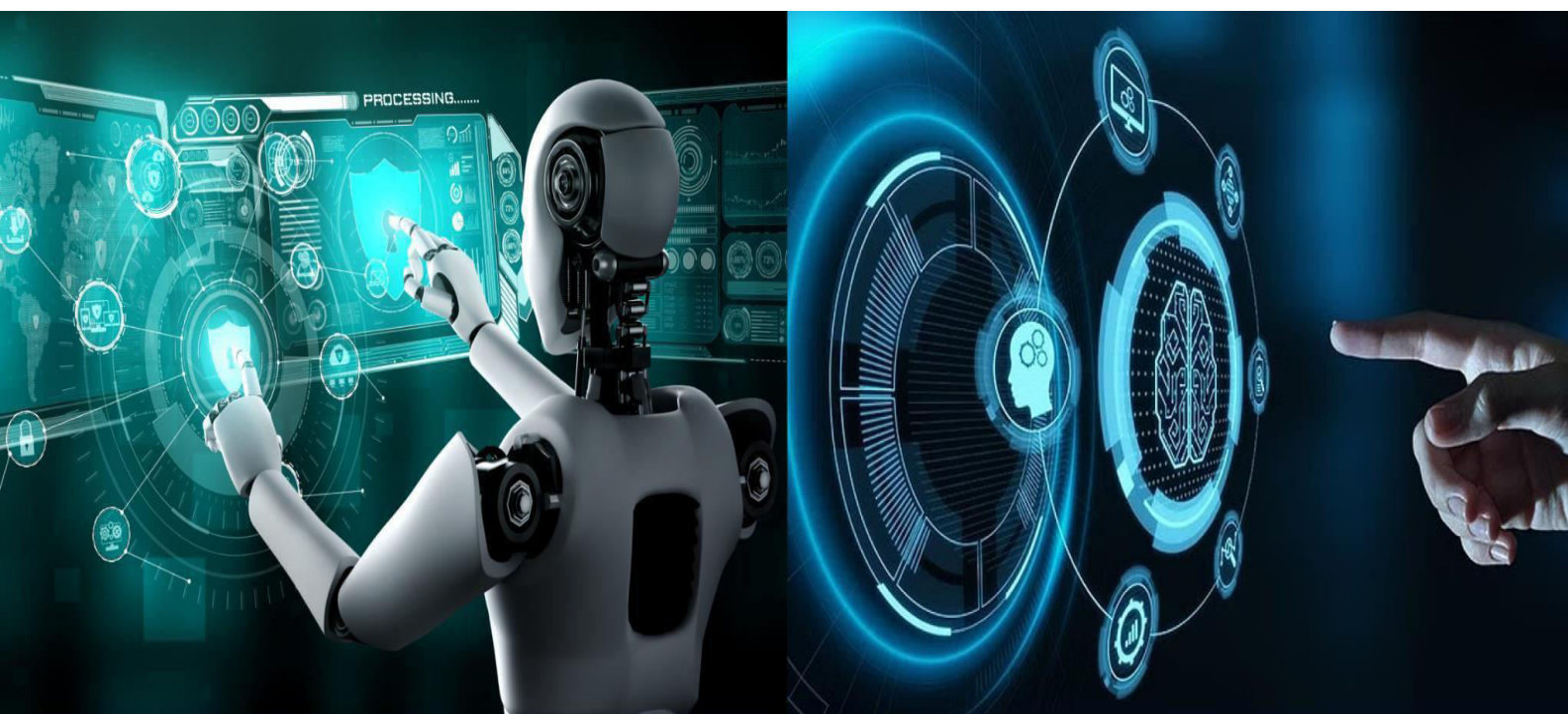


International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

AI Based Intrusion Detection Device

Sourabh D¹, Dr.Malatesh S H², Shinde Radha³, Shweta⁴, Yashwant Gowda⁵

Dept. of Computer Science and Engineering, MS Engineering College, Bengaluru, Karnataka, India¹

Professor& HOD, Dept. of Computer Science and Engineering, MS Engineering College, Bengaluru, Karnataka, India²

Dept. of Computer Science and Engineering, MS Engineering College, Bengaluru, Karnataka, India³

Dept. of Computer Science and Engineering, MS Engineering College, Bengaluru, Karnataka, India⁴

Dept. of Computer Science and Engineering, MS Engineering College, Bengaluru, Karnataka, India⁵

ABSTRACT: Security plays a crucial role in residential, institutional, and commercial environments, particularly with the rising occurrences of unauthorized entry and theft. Traditional security mechanisms such as locks, CCTV surveillance, and manual monitoring lack automated real-time intelligence and cannot identify individuals. This paper proposes an AI-based intrusion detection device built using Raspberry Pi, Pi Camera, OpenCV, and IoT communication. The system employs the Haar Cascade classifier for face detection and the Local Binary Pattern Histogram (LBPH) algorithm for face recognition. If a person is identified as an authorized user, the door unlocks automatically through a relay-controlled solenoid lock. If the person is unknown, the system captures an image and immediately sends it to the owner via a Telegram bot. Experimental evaluation demonstrates efficient detection accuracy, fast response time, and reliable performance under normal indoor lighting. The system provides a low-cost, autonomous, and scalable approach to intelligent intrusion detection and real-time access control.

KEYWORDS: intrusion detection, Raspberry Pi, LBPH, Telegram bot, face recognition, smart security

I. INTRODUCTION

Security systems have evolved significantly from traditional manual methods to automated systems driven by Artificial Intelligence (AI) and Internet of Things (IoT). Manual locks, CCTV systems, and security guards offer limited proactive monitoring and rely heavily on human intervention. They lack the capability to differentiate between authorized and unauthorized individuals, limiting their effectiveness.

Recent advancements in AI-based computer vision allow real-time face detection and recognition using lightweight models on embedded platforms. Raspberry Pi, paired with OpenCV, provides a cost-effective and efficient platform suitable for implementing intelligent access control systems. This research presents an AI-based intrusion detection device that performs automated face recognition and intrusion alerting. Using Raspberry Pi 4, Pi Camera, OpenCV Haar Cascade, LBPH model, and Telegram bot integration, the system identifies authorized personnel and alerts administrators instantly about unknown individuals. In conclusion, the AI Intrusion Detection Device represents a modern, automated, and reliable approach to safeguarding property and assets. Its ability to detect, recognize, alert, and control access makes it an innovative and effective solution for residential, commercial, and industrial security challenges.

II. MATERIALS AND METHODS

This section provides an overview of the key components, system architecture, and algorithmic workflow implemented to develop the AI-based intrusion detection device, highlighting how hardware, software, and intelligent recognition techniques work together to ensure real-time security and automated threat response.

A. System Overview

The system continuously monitors the entrance using a Pi Camera, performs face detection and recognition, and takes appropriate action. The Raspberry Pi functions as the core processing unit, integrating vision algorithms, relay control, door lock, sd card and IoT communication.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

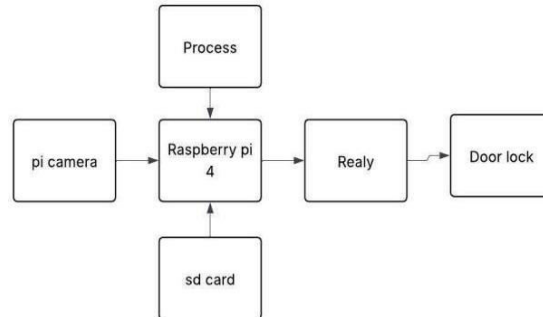


Fig.1: System Architecture of the Proposed Intrusion Detection Device

The architecture includes the following modules:

- Pi Camera for video capture
- Raspberry Pi for AI processing
- Haar Cascade for face detection
- LBPH for face recognition
- Relay driver for lock control
- Solenoid lock for physical access
- Telegram bot for notifications

The block diagram shows the integrated system Architecture flow: the camera captures video, the Raspberry Pi analyzes it using AI, and based on recognition results, the system either grants access through a relay-controlled lock or sends instant Telegram alerts for unauthorized users, ensuring smart and secure intrusion detection.

B. Data Flow Diagram

The flowchart represents the complete operational workflow of the AI-based intrusion detection device. The system begins by initializing the camera, loading the AI recognition model, and activating the Telegram bot. Once initialized, the camera continuously monitors the environment and detects faces using the Haar Cascade algorithm. If a face is detected, the system proceeds to the recognition stage, where the LBPH (Local Binary Patterns Histogram) algorithm identifies whether the person is authorized or unknown.

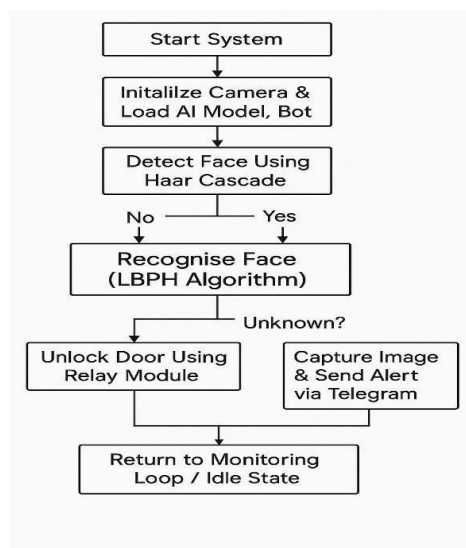


Fig.2: Data Flow Diagram of the Face Recognition System



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

If the detected face matches an authorized user, the system triggers the relay module to unlock the door, granting secure access. Conversely, if the face is classified as unknown, the device immediately captures an image of the intruder and sends an alert notification to the user through Telegram, ensuring rapid response to potential threats. After completing the respective action, the system returns to its monitoring loop or idle state, maintaining continuous security surveillance.

C. Sequence Diagram

The sequence diagram illustrates the interaction between the user, hardware components, and software modules during the intrusion detection process. When a user approaches the door, the camera captures a live frame and sends it to the AI model for processing. The AI model forwards the frame to the recognition module, where face detection is performed, followed by face recognition using the LBPH algorithm. If the system identifies the individual as a known and authorized user, the recognition module signals the relay module to unlock the door, allowing secure entry. On the other hand, if the person is classified as unknown, the recognition module communicates with the Telegram bot to send an immediate alert notification to the owner, ensuring quick awareness of potential intrusions. After completing the appropriate action—unlocking the door or sending an alert—the system returns to the monitoring state, ready to process the next interaction.

This sequence demonstrates how each component collaboratively enables automated, intelligent, and real-time intrusion detection.

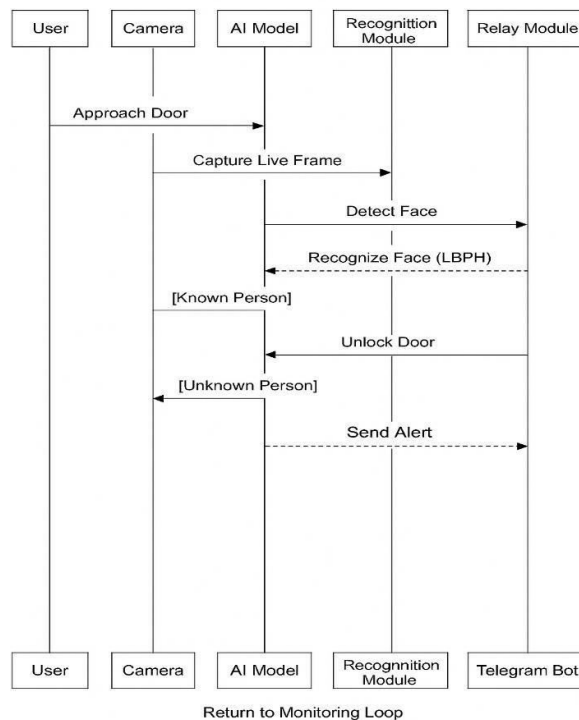


Fig.3: Sequence Diagram of Intrusion Detection and Response

D. Hardware Implementation

The hardware setup for the AI-based intrusion detection device integrates key electronic components required for real-time monitoring and automated access control. At the core of the system is the Raspberry Pi, which serves as the primary processing unit responsible for executing the AI model, handling camera input, and controlling peripheral modules. A Raspberry Pi Camera Module, connected via the CSI interface, is used to continuously capture live video frames for face detection and recognition.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

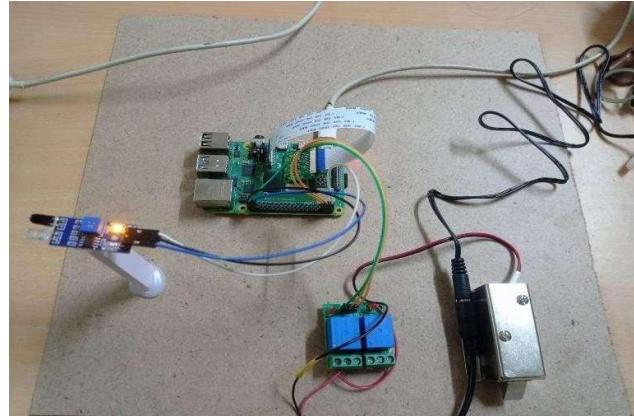


Fig.4: Hardware Implementation Setup

An infrared obstacle/IR sensor is incorporated to detect motion or the presence of an approaching user, which helps in activating the camera and optimizing system responsiveness. For access control, a relay module is connected to the Raspberry Pi's GPIO pins. This relay controls the electromagnetic door lock, enabling the system to unlock the door when an authorized face is recognized. The lock receives power from an external supply, ensuring stable operation independent of the Raspberry Pi's power constraints. All components are interconnected using jumper wires and powered through stable DC sources. This modular hardware arrangement ensures reliability, safety, and ease of integration, forming the foundation for the intelligent intrusion detection and access control system.

E. Software Operation

1. Initialization of Pi Camera and Haar Cascade: The software begins by initializing the Raspberry Pi Camera module and loading the Haar Cascade classifier for face detection. This ensures that the system is ready to capture video frames and detect facial features in real time.
2. Continuous Video Frame Capture: Once initialized, the system enters a continuous loop where live video frames are captured from the Pi Camera. These frames serve as the input for the subsequent detection and recognition processes.
3. Face Detection: Each captured frame is processed using the Haar Cascade detection algorithm to identify the presence and location of faces. Only frames containing faces are forwarded for the recognition stage, optimizing system performance.
4. Identity Prediction Using LBPH Algorithm: If a face is detected, the Local Binary Patterns Histogram (LBPH) recognition model is applied to predict the identity. The algorithm compares the detected face with a trained dataset of authorized users and returns an identity label along with a confidence score.
5. Relay Control for Authorized Users: For recognized and authorized users, the software triggers the relay module through the Raspberry Pi GPIO pins. This action activates the electromagnetic lock, allowing secure access to the door.
6. Telegram Alert for Intruders: If the detected face does not match any authorized identity, the system classifies the person as an intruder. In this case, the software captures an image and sends an instant alert to the owner via Telegram, ensuring immediate notification of a security breach.

F. System Testing

System testing was carried out to verify that the AI-based Intrusion Detection Device performs correctly, reliably, and efficiently under real-world conditions. Multiple testing methods were applied to ensure that both functional and non-functional requirements were met.

1. Unit Testing: Individual modules such as image capture, face detection, LBPH recognition, relay control, Telegram API, and GUI components were tested independently to ensure correct functionality before integration.
2. Integration Testing: Modules were combined and tested together to validate complete workflows, including authorized recognition leading to relay activation and unknown detection leading to Telegram alerts. This ensured smooth interaction between the camera, GPIO, and network components.
3. System Testing: The fully integrated system was tested in real-time conditions to evaluate detection speed,



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

recognition accuracy, door unlocking reliability, alert delivery time, and camera performance in varying lighting environments.

4. Performance Testing: Key performance parameters such as recognition time (<1 sec), Telegram delay (2– 3 sec), frame rate (10–15 FPS), and accuracy under different conditions were measured to assess system efficiency.
5. Security Testing: Attempts were made to bypass the system using unregistered faces, false inputs, and unauthorized access. The system successfully restricted access, indicating strong security robustness.
6. User Interface Testing: GUI elements for dataset creation, image capture, training, verification, and live testing were evaluated for usability and ease of navigation.
7. Stress Testing: The system was operated continuously for 2 hours, subjected to repeated recognitions and rapid relay switching. It remained stable without performance degradation.

Requirement	Expected Result	Actual Result	Status
Face detection	Detect faces in real time	Achieved	Pass
Face recognition	Identify authorized users accurately	Achieved	Pass
Intruder detection	Unknown faces trigger alert	Achieved	Pass
Telegram alert	Send message + image instantly	Achieved	Pass
Door unlocking	Unlock only for authorized users	Achieved	Pass
GUI usability	Easy to operate	Achieved	Pass
System stability	Run 24×7	Achieved	Pass
Response time	< 1 second	Achieved	Pass

G. Performance Evaluation

The performance of the AI-based intrusion detection system was evaluated in terms of detection accuracy, recognition accuracy, response time, and overall system stability. Experimental testing was conducted under typical indoor lighting conditions to assess the system’s reliability during real-world operation.

1. Detection and Recognition Accuracy: The system demonstrated reliable face detection performance, achieving an accuracy range of 85–95%, depending on lighting and distance. The LBPH-based face recognition module provided an accuracy of 88–92%, showing strong consistency in identifying authorized users. These results confirm the suitability of LBPH for lightweight, edge-based facial recognition on Raspberry Pi.
2. Response Time: The system responded efficiently during real-time operation. Face recognition was completed in less than 1 second, enabling quick decision-making for access control. For intrusion events, the Telegram alert mechanism delivered notifications within 2–3 seconds, providing timely warnings to the user through the Telegram Bot API.
3. System Stability: To evaluate long-term performance, the system was operated continuously for 2 hours. During this period, no overheating, lag, or performance degradation was observed. Both hardware and software modules remained stable, demonstrating the system’s reliability for continuous monitoring applications.

Parameter	Value	Remarks
Detection Accuracy	90%	Good indoor lighting
Recognition Accuracy	85%	Using LBPH
Telegram Delay	2–3 seconds	Stable network
Relay Response Time	0.5 second	Consistent operation



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Parameter	Result
CPU Temperature	Stable (60–65°C)
Memory Usage	Moderate
Frame Rate Drop	None
Crashes	None
Relay Heating	None

Distance	Performance
1 meter	Excellent
1.5 meters	Good
2 meters	Fair
Above 2 meters	Poor detection

III. CONCLUSIONS

The AI-Based Intrusion Detection Device developed in this project demonstrates the successful integration of Artificial Intelligence, image processing, IoT communication, and automation into a unified, intelligent security system. Unlike traditional security methods such as manual locks, CCTV surveillance, and basic alarm systems the proposed solution provides proactive monitoring and the ability to identify individuals in real time, thereby overcoming limitations of human dependency and delayed response. By leveraging the Raspberry Pi and Pi Camera, the system performs real-time face detection and recognition using the Haar Cascade classifier and LBPH algorithm. It accurately identifies authorized users and automatically unlocks the door, offering seamless and secure access without manual intervention. This enhances both convenience and safety. For unauthorized or unknown individuals, the system captures their image and immediately sends an alert via Telegram, enabling remote, instant awareness of potential security threats. The Telegram bot also supports remote control capabilities, giving users the flexibility to operate the system from any location. The integration of reliable hardware components including the relay module, solenoid lock, and IR sensor ensures efficient physical access control. Continuous operation with low power consumption further establishes the system’s suitability for 24×7 automated surveillance. Performance evaluations confirm its high accuracy, fast response time, stability, and real-world practicality. Overall, the project demonstrates that a low-cost AI-driven intrusion detection system can deliver advanced security features typically found only in high-end commercial solutions. It showcases the potential of embedded AI systems and provides a scalable foundation for enhancements such as deep-learning-based recognition, cloud dashboards, multi-camera setups, and hybrid authentication. The system fulfills its objectives as a smart, secure, automated, and user-friendly solution suitable for homes, offices, institutions, laboratories, and industrial environments.

REFERENCES

1. Viola P., Jones M., “Rapid Object Detection using a Boosted Cascade of Simple Features,” IEEE CVPR.
2. OpenCV, “Face Detection and Recognition Documentation,” 2025.
3. Raspberry Pi Foundation, “Raspberry Pi 4 Model B Technical Specifications,” 2024.
4. Telegram API, “Bot Communication and Image Handling Documentation,” 2025.
5. Pecolt S. et al., “Biometric Recognition Systems for Embedded Platforms,” MDPI, 2025.
6. Guerbaoui M., “Advanced Facial Recognition on Edge Devices,” E3S Conferences, 2025.
7. Aboluhom, A. A., et al., “Face Recognition using Transfer Learning Techniques on Embedded Raspberry Pi Systems,” Oxford University Press (OUP), 2024.
8. S. Maryam & R. Al-Hyari, “Real-Time Intrusion Detection using Edge AI and IoT-based Alert Systems,” IEEE Internet of Things Journal, 2023.
9. Kadambi S., “Smart Surveillance Systems: AI-driven Face Recognition for Secure Access Control,” Elsevier Journal of Smart Security, 2024.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details