IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, April 2025
Impact Factor: 7.67

Secure Door Lock System Using AI and IoT

Renuka Sanjay Kurhade[1] and Pratiksha Rajesh Mohite[2]
Department of Computer Applications[1-2]
S. M. Joshi College, Hadapsar, Pune, India

Abstract: *In this project, we propose a smart door lock system that utilizes face recognition technology for secure access control. The system captures human images and compares them with stored images in a database to authenticate users. The primary objective is to enhance home security by implementing an AI-powered access control system using Python and the OpenCV library. Face recognition is widely used in security and law enforcement applications due to its ability to identify individuals in images, videos, or real-time environments. This paper discusses the development of an automated locking system integrated with a 12V solenoid electronic lock, leveraging ESP32-CAM and OpenCV to improve accuracy and effectiveness.*

Keywords: Python, OpenCV, Face Recognition, Security, Microsoft Visual Studio Code

I. INTRODUCTION

Face recognition is a widely used biometric identification method, particularly in security applications. The ability to distinguish individuals based on facial features makes it a reliable alternative to traditional security systems such as keycards, passwords, or fingerprint scanning. This paper presents a survey on face recognition techniques using Python and OpenCV and discusses the development of a security access control system integrated with an electronic lock. The system enhances home security by allowing authorized users to unlock doors automatically.

II. OBJECTIVE

- To develop a secure door lock system using face recognition for access control.
- To implement automatic locking and unlocking of doors using ESP32-CAM.
- To enhance home security with AI-based technologies.

III. LITERATURE REVIEW

Several studies have explored face recognition for security applications:

- **Mayank Agarwal (2021)** proposed a high-accuracy face recognition model using Eigenfaces.
- **M.M. Krishna** developed a door unlocking system using Raspberry Pi for image verification.
- **B. Manigandan** utilized LabVIEW for face recognition but encountered high costs due to MYRIO components.
- **G. Kaviyasanthosh** reviewed biometric methods and selected Python and OpenCV for their accuracy and adaptability to facial feature changes.

IV. DATA COLLECTION

Objective:
To analyze the impact of environmental factors on facial recognition accuracy.

Data Points:

- Lighting: Daylight, low light, artificial lighting variations.
- Weather Conditions: Performance under rain, fog, or snow
- Obstructions: Faces with masks, scarves, or accessories.

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, April 2025
Impact Factor: 7.67

Sources: Google Scholar, IEEE Xplore, government websites for statistical data on facial recognition performance under different conditions.

V. EXISTING SYSTEM AND LIMITATIONS

Traditional security systems rely on physical keys, passwords, or keycards, which are vulnerable to theft, loss, and hacking. Biometric authentication, particularly face recognition, overcomes these limitations by ensuring secure and seamless access control.

Advantages:

- Eliminates the need for physical keys.
- Harder for intruders to bypass.
- Enhances security for vulnerable individuals (children, elderly, disabled).
- Can integrate with smartphones for remote access.

Limitations:

- Vulnerable to app failures or hacking attempts.
- Requires high storage capacity for facial data.

VI. PROBLEM STATEMENT

Security is a crucial aspect of modern living, requiring reliable authentication methods. The proposed system enhances door security using face recognition, minimizing risks associated with lost keys or stolen passwords. However, potential privacy concerns related to biometric data collection must be addressed.

VII. SYSTEM DESIGN AND REQUIREMENT ANALYSIS

A. Software Requirements:

Arduino IDE 1.8.12 for ESP32-CAM programming.

B. Hardware Requirements:

- ESP32-CAM – A camera module with Wi-Fi and Bluetooth for facial recognition.
- UART TTL Programmer – Connects USB to serial UART for programming ESP32-CAM.
- Relay Module (5V) – Enables automatic circuit switching.
- 12V Solenoid Lock – Activates upon voltage signal, securing the door.
- LED Indicators – Displays system status.
- 7805 Voltage Regulator – Maintains 5V output for stability.
- 100uF 16V Capacitor – Filters noise and ensures smooth operation.
- Breadboard and Jumper Wires – Prototyping and circuit connections.
- GSM Module – Sends alerts via SMS for unauthorized access.

VIII. IMPLEMENTATION METHODOLOGY

- **Face Detection:** The system captures live facial images using ESP32-CAM.
- **Feature Extraction:** OpenCV's face recognition module processes the image.
- **Database Matching:** The extracted features are compared with stored images.
- **Access Control:** If a match is found, the solenoid lock is triggered.
- **Alert Mechanism:** Unauthorized access attempts trigger an SMS alert via the GSM module.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, April 2025
Impact Factor: 7.67

IX. FUTURE SCOPE

- Integration with CCTV for enhanced monitoring.
- Expansion to industrial security and high-security bank vaults
- Additional security features like voice recognition.
- Real-time alerting via mobile apps for remote access control.

X. CONCLUSION

The proposed smart door lock system enhances security using AI and IoT technology. By implementing face recognition, we eliminate the need for physical keys and passwords, reducing security risks. Future improvements can enhance system reliability and expand its applications to various sectors.

REFERENCES

[1]. Zhang, X., et al. (2022). "Deep Learning for Face Recognition: Advances and Future Trends." *IEEE Transactions on Pattern Analysis and Machine Intelligence.*

[2]. Parkhi, O. M., et al. (2015). "Deep Face Recognition." *British Machine Vision Conference (BMVC).*

[3]. Ahonen, T., Hadid, A., &Pietikainen, M. (2006). "Face Recognition with Local Binary Patterns." *IEEE Transactions on Pattern Analysis and Machine Intelligence.*

[4]. Viola, P., & Jones, M. (2001). "Robust Real-Time Face Detection." *International Journal of Computer Vision.*