www.ijarp.com ISSN 2456-9992 Page: 01-06
International Journal Advanced Research Publications
Research Article
Volume: 02
Issue: 05

A REAL-TIME AI-BASED FACE RECOGNITION SMART ACCESS CONTROL SYSTEM WITH IOT HARDWARE INTEGRATION

***Ayush Kumar, Vishal Upmanu**

Department of Computer Science and Engineering, RD Engineering College, Ghaziabad, U.P., India-201206.

Article Received: 21 March 2026, Article Revised: 11 April 2026, Published on: 01 May 2026

***Corresponding Author: Ayush Kumar**
Department of Computer Science and Engineering, RD Engineering College, Ghaziabad, U.P., India-201206.
DOI: https://doi-doi.org/101555/ijarp.7118

ABSTRACT

With the growing demand for intelligent security infrastructure, conventional access control systems such as mechanical locks, RFID cards, and PIN-based authentication mechanisms have proven vulnerable to duplication, theft, and misuse. This research presents **IntelliGate**, a real-time Artificial Intelligence (AI)-driven facial recognition-based smart access control system integrated with IoT-enabled hardware components. The system utilizes computer vision algorithms implemented through OpenCV and facial encoding techniques powered by Dlib to authenticate individuals. Upon successful identification, a Raspberry Pi Foundation-developed Raspberry Pi 4 activates a relay module connected to an electromagnetic lock. Unauthorized access attempts trigger automated logging, image capture, buzzer alerts, and real-time email notifications.

Experimental analysis demonstrates an average recognition accuracy of approximately 94% with low response latency, making IntelliGate a scalable, cost-effective, and intelligent security solution for residential, institutional, and industrial applications.

KEYWORDS: Face Recognition, IoT Security, Artificial Intelligence, Smart Gate System, Computer Vision, Embedded Systems.

1. INTRODUCTION

Security is a foundational requirement in smart cities, educational institutions, residential societies, and corporate environments. Traditional security systems depend on possession-

based authentication (keys, RFID cards) or knowledge-based authentication (PINs, passwords). These methods are prone to compromise and unauthorized sharing.

Biometric authentication provides a more secure and identity-specific solution. Among various biometric technologies—such as fingerprint recognition, iris scanning, and voice recognition—facial recognition stands out due to its contactless, non-intrusive, and user-friendly nature.

Recent advancements in Artificial Intelligence and Deep Learning have significantly enhanced the reliability of facial recognition systems. However, many implementations remain limited to software prototypes without real-time physical hardware integration.

This paper proposes **IntelliGate**, a complete AI–IoT integrated access control system capable of:

- Real-time facial authentication
- Automated gate unlocking via hardware interface
- Unauthorized attempt detection and alerting
- Digital logging and monitoring

2. Literature Review

The concept of automated face recognition was popularized by the Eigenfaces method introduced by Turk and Pentland. Later, Viola–Jones object detection algorithms improved real-time face detection capabilities. Modern machine learning libraries such as OpenCV and Dlib further enhanced performance by enabling high-accuracy feature extraction.

IoT-based smart security systems commonly utilize embedded platforms like Raspberry Pi 4 for hardware interfacing. Previous systems have implemented RFID-based smart locks or fingerprint-based authentication, but these require physical interaction or possession of a device.

IntelliGate differs by integrating:

- Contactless biometric authentication
- Embedded hardware automation
- Real-time email notification system
- Edge-based processing without cloud dependency.

This integration ensures faster response, improved privacy, and reduced operational costs.

3. System Architecture

The IntelliGate system is divided into two major subsystems:

3.1 Software Layer

1. Video Capture Module
2. Face Detection Module
3. Feature Encoding Module
4. Matching and Classification Module
5. Event Logging System
6. Notification Module
7. Web Dashboard Interface

3.2 Hardware Layer

- USB HD Camera
- Raspberry Pi 4
- 5V Relay Module
- Electromagnetic Door Lock
- Buzzer
- Power Supply Unit

The architecture ensures seamless interaction between AI-based recognition and IoT-based physical control.

4. PROPOSED METHODOLOGY

4.1 Image Acquisition

The system captures live video frames using a USB camera connected to the Raspberry Pi.

4.2 Face Detection

The Viola–Jones Haar Cascade classifier provided by OpenCV detects faces in real time.

4.3 Feature Extraction

Each detected face is converted into a 128-dimensional embedding vector using deep metric learning models from Dlib.

4.4 Face Matching Algorithm

The Euclidean distance between stored face encodings and the detected encoding is calculated:

$$d = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$$

If:

- If distance < threshold → Authorized
- Else → Unauthorized.

4.5 Hardware Execution Logic

If authorized:

- GPIO pin set HIGH
- Relay module activated
- Electromagnetic lock opens for 5 seconds
- Automatic re-lock after timeout

If unauthorized:

- Image captured
- Log entry stored in database
- Email notification sent
- Buzzer activated

5. Hardware Integration

The Raspberry Pi 4 serves as the central controller. GPIO pins interface with the relay module, which controls the power circuit of the electromagnetic lock.

5.1 Operational Flow:

1. Face recognized
2. GPIO signal transmitted
3. Relay switches ON
4. Lock disengages
5. System auto-locks after delay

The average hardware activation delay was measured below 0.5 seconds, ensuring near real-time operation.

6. Experimental Results

Testing was conducted under varying lighting conditions and user angles.

6.1 Performance Metrics

Parameter	Observed Value
Recognition Accuracy	~94%
Average Response Time	1.3 sec
False Acceptance Rate	3%
False Rejection Rate	3%
Hardware Latency	< 0.5 sec

6.2 Observations

- Slight accuracy drop in low-light conditions
- Improved recognition with higher camera resolution
- Stable performance for up to 20 registered users

7. DISCUSSION

The integration of AI and IoT in IntelliGate demonstrates the feasibility of real-time biometric access control. Compared to conventional systems, IntelliGate:

- Eliminates physical keys and RFID cards
- Reduces unauthorized duplication risks
- Enables digital logging and traceability
- Provides instant remote alerts
- Maintains privacy via edge processing

The cost efficiency of Raspberry Pi-based deployment makes the system highly adaptable for educational institutions, offices, and smart homes.

8. CONCLUSION AND FUTURE SCOPE

8.1. Conclusion

This research introduced IntelliGate, a real-time AI-driven face recognition access control system integrated with IoT hardware. The system successfully bridges the gap between intelligent biometric authentication and automated physical gate control.

Experimental evaluation confirms high recognition accuracy and minimal response latency. IntelliGate provides a secure, scalable, and affordable smart security solution aligned with modern digital infrastructure requirements.

8.2. Future Scope

Future developments may include:

- Cloud-synchronized face database

- Mobile application integration
- Mask detection and liveness detection
- Multi-factor authentication (Face + OTP)
- Edge AI model optimization
- Smart home ecosystem integration

REFERENCES

1. G. Bradski, "The OpenCV Library," Dr. Dobb's Journal, 2000.
2. Goodfellow et al., *Deep Learning*, MIT Press, 2016.
3. Raspberry Pi Foundation, "Raspberry Pi 4 Documentation," 2023.
4. M. Turk and A. Pentland, "Eigenfaces for Recognition," 1991.
5. P. Viola and M. Jones, "Rapid Object Detection," 2001.
6. D. E. King, "Dlib-ml: A Machine Learning Toolkit," 2009.
7. K. Jain et al., "An Introduction to Biometric Recognition," IEEE, 2004.
8. S. Kumar and A. K. Singh, "Smart Security Systems using IoT," 2020.
9. Kiran, Dharamveer Singh, NitinGoyal, (2023) "Analysis Of How Digital Marketing Affect By Voice Search", Journal of Survey in Fisheries Sciences, Vol. 30 (2) 407-412. https://doi.org/10.53555/sfs.v10i3.2890
10. YuktiTyagi, Dharamveer Singh, Ramander Singh, SudhirDawra (2024) "Analysis Of The Most Recent Trojans On The Android Operating System", Educational Administration: Theory and Practice, Vol. 30(2) 1320-1327. https://doi.org/10.53555/kuey.v30i2.6846
11. Shivanee Singh, Dharamveer Singh, RavindraChauhan (2023) "Manufacturing Industry: A Sustainability Perspective On Cloud And Edge Computing", Journal of Survey in Fisheries Sciences, pp 1592-1598. https://doi.org/10.53555/sfs.v10i2.2889
12. Ungermann, F., Kuhnle, A., Stricker, N. and Lanza, G., 2019. Data Analytics for Manufacturing Systems–A Data-driven Approach for Process Optimization. Procedia CIRP, 81, pp.369-374.
13. Azahara. 2016. How Data mining is used to generate Business Intelligence. Geographica. [online] retrieved from http://www.blog-geographica.com/2016/11/15/how-data-mining-is-used-to-generate-business-intelligence/ [Accessed on 3 march 2021]