iJRASET
International Journal For Research in Applied Science and Engineering Technology



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 14 **Issue:** V **Month of publication:** May 2026

**DOI:** https://doi.org/10.22214/ijraset.2026.81744

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue V May 2026- Available at www.ijraset.com*

# Facial Recognition Attendance System

Prof. A. D. Dudhe[1], Priyanka Jaysing Rathod[2], Deep Pravin Lukka[3], Durgesh Govindrao Hemne[4], Raj Chandu Gavali[5]
*Electronics and Telecommunication Department, Jagadambha Collage of engineering and Technology Yavatmal*

***Abstract:*** ***Facial Authentication System is a biometric technology that identifies or verifies a person using facial features. This research focuses on designing a secure and efficient authentication system using computer vision and machine learning techniques. The system captures facial images, detects faces, extracts unique features, and compares them with stored data for authentication. The proposed system aims to provide high accuracy, fast processing, and enhanced security compared to traditional methods like passwords or ID cards.***

***The Face Recognition Attendance System represents an innovative solution at the intersection of artificial intelligence and attendance management. Leveraging Python open-source libraries such as OpenCV and NumPy, alongside machine learning techniques, the system aims to streamline the attendance tracking process.***

***By employing face detection algorithms and feature extraction methods, the system identifies individuals, records their attendance, and updates the database in real-time. The system architecture incorporates components like a front-end web application, real-time prediction module, registration form module, reporting module, Redis database, Streamlit framework, Insightface library, and AWS deployment. Through continuous improvement and innovation, the system enhances user experience, accuracy, and efficiency in attendance management.***

***Facial recognition technology has emerged as a vital component in modern security systems. This paper presents the design and implementation of a low-cost, real-time facial recognition and tracking system using an Arduino microcontroller, a USB camera, and Python-based image processing. The system captures live video, detects faces using the OpenCV library, and compares them against a pre-stored database. Upon successful recognition, the Arduino triggers an output device such as a servo-controlled door lock or an alarm. The proposed system demonstrates that affordable hardware can be integrated with open-source software to achieve reliable facial authentication for small-scale security applications.***

***Keywords: Facial Recognition, Arduino, OpenCV, Real-Time Tracking, IoT Security, Image Processing, Attendance System, Machine Learning, Insightface.***

## I. INTRODUCTION

With the rapid growth of digital systems, secure authentication has become essential. Traditional methods such as passwords and PINs are vulnerable to theft and misuse. Facial authentication offers a contactless, user-friendly, and secure alternative. It uses unique facial characteristics that are difficult to duplicate. This research paper presents the development of a facial authentication system using image processing and machine learning algorithms.

Facial recognition is a biometric method that identifies individuals based on unique facial features. While high-end systems rely on powerful processors and expensive cameras, there is a growing need for low-cost, portable, and energy-efficient solutions for small businesses, homes, and IoT applications. This research explores the feasibility of implementing a facial recognition system using an Arduino microcontroller as the control unit, combined with a Pythonbased image processing module running on a connected computer or Raspberry Pi.

A facial recognition system using Arduino is an embedded project that combines computer vision with microcontroller-based control to identify or verify a person's identity based on their facial features. It integrates image processing algorithms (often via Python and OpenCV) with Arduino's hardware control capabilities, enabling automation, security, and personalized interactions.

In today's dynamic organizational environments characterized by evolving workflows and technological advancements, the demand for streamlined and accurate attendance management has never been more pronounced. Manual methods of attendance tracking, reliant on paper-based registers or cardswipe systems, not only entail significant labor but also are prone to errors, resulting in discrepancies in attendance records and impeding effective decision-making processes. Moreover, the introduction of the AI Based Face Recognition Attendance System signifies more than just a technological advancement; it underscores a commitment to fostering a culture of innovation and efficiency within organizations. By embracing cutting-edge technologies, organizations can unlock new avenues for growth, optimize operational processes, and maintain a competitive edge in today's rapidly evolving landscape.

©IJRASET: All Rights are Reserved 

## II. PURPOSE

The main purpose of the Facial Authentication System is to develop a secure, reliable, and efficient method for verifying the identity of individuals using their facial features. Traditional authentication methods such as passwords, PINs, and ID cards have several limitations, including the risk of being forgotten, stolen, or misused. This project aims to overcome these issues by implementing a biometricbased authentication system that is both user-friendly and highly secure.

Another important purpose of this project is to provide a contactless authentication solution, which is especially useful in environments where hygiene and safety are important. By using facial recognition technology, the system eliminates the need for physical contact, making it suitable for modern applications.The project ases on improving accuracy and speed in the authentication process. By using advanced image processing and machine learning techniques, the system is designed to quickly detect and recognize faces in real-time, ensuring minimal delay and high performance.

Additionally, this project aims to explore the practical implementation of computer vision concepts and machine learning algorithms. It helps in understanding how theoretical knowledge can be applied to realworld problems such as security, surveillance, and identity verification.

Finally, the purpose of this system is to provide a scalable solution that can be used in various applications such as attendance systems, mobile authentication, banking security, and access control systems. The project also lays a foundation for future enhancements, including integration with deep learning models and cloud-based systems for improved performance and security.

1) Security & Access Control: To allow only authorized individuals to access a device, room, or system by verifying their face. Acts as a biometric authentication method, reducing the risk of password theft or key duplication duplication.
2) Automation & Personalization: Can trigger personalized actions when a recognized face is detected (e.g., adjusting lighting, doors, or greeting the user).
3) Learning & Experimentation: Helps students, hobbyists, and researchers understand the integration of computer vision (OpenCV) with microcontrollers (Arduino). Encourages hands-on experience with image processing, machine learning, and IoT concepts.
4) Cost-Effective Prototyping: Demonstrates how low-cost hardware can be combined with software to create functional biometric systems without expensive commercial solutions.

## III. OBJECTIVE OF SYSTEM

The main objective of this research is to develop an innovative Face Recognition-Based Attendance System that utilizes real-time data to capture attendance in a seamless and reliable manner. The system aims to reduce administrative burdens, enhance accountability, and optimize the overall attendance management process.

## IV. LITEREIVEW REVIEW

Aditya Umalkar, © 2023 IJCRT | Volume 11, Issue 8 August 2023 | ISSN: 2320-2882

In the past, attendance was manually recorded, which takes a lot of time and frequently results in mistakes. In addition, there are a lot of questions about where the information on attendance come from; in reality, most attendance statistics are not obtained from genuine situations. It is no longer possible to take student attendance using the outdated approach of using paper sheets. According to the research, there are numerous ways to address this problem. A research journal titled "Attendance System Using NFC Technology with Embedded Camera on Mobile Device" by Bhise, Khichi, Korde, and Lokare (2015) suggests that an attendance system can be improved by using Near Field Communication (NFC) technology and a mobile application. The system involves assigning each student a unique NFC tag during their enrolment into the college. The professor then records the students' faces on their cell phone's embedded camera by touching or moving these tags. To validate and verify the data, it is forwarded to the college server. This method is useful since it makes connection establishment simple and quick, which expedites the attendance-taking procedure.

Rasika Rajiv Choudhari, © 2025 IJRTI | Volume 10, Issue 11 November 2025 | ISSN: 2456-3315 The progression of attendance management systems reflects broader trends in information technology adoption, biometrics, and AI. Early systems relied on manual processes—roll calls, sign-in sheets, or physical tokens— characterized by low efficiency and high susceptibility to error and manipulation , Subsequent adoption of electronic and card-based methods, such as Radio Frequency Identification (RFID) cards and smart tokens, improved operational efficiency but introduced new vulnerabilities, including proxy misuse and card swapping . The shift to biometric systems marked a significant advance, leveraging unique physiological or behavioral characteristics for identification. Fingerprint and iris recognition systems provided higher accuracy and reduced the risk of proxy attendance. However,

these methods raised concerns over hygiene, user acceptance, and operational practicality, especially in largescale deployments or during public health crises.

Y. Kortli .Group I Journal Research Journal ISSN : 2347-7180 Vol-13, Issue-2, No. 4, February 2023 During the characteristic extraction stage, the phase takes into account the characteristics extracted from the background and matches them to the familiar faces stored in a specific database. There are two basic applications of FR, the first is known as verification, while the second is known as identification. At the time of the identification step, a test face is compared to a collection of faces intended for finding the most likely match. Now, in the step of identification, a test face is compared to a face that is known in the database to determine whether it should be rejected or accepted.

## V. METHODOLOGY

The methodology of the Facial Authentication System describes the step-by-step process used to design, develop, and implement the system. It involves image acquisition, face detection, feature extraction, face recognition, and authentication. The overall process ensures accurate and real-time identification of individuals.

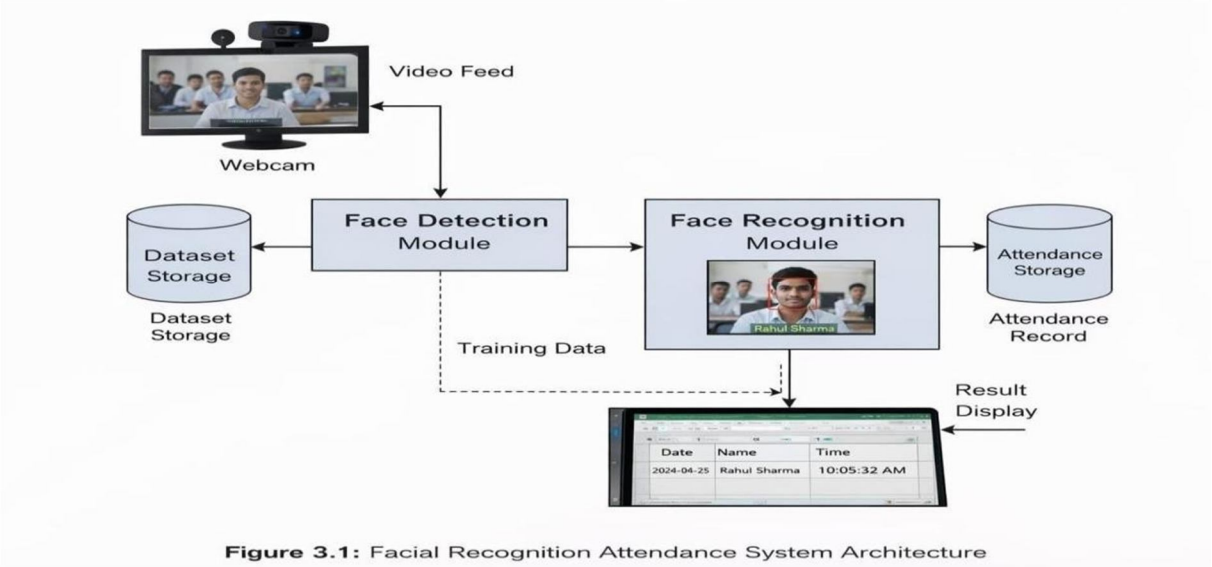



**Figure 3.1:** Facial Recognition Attendance System Architecture

### *A. Image Acquisition*

The first step in the system is capturing facial images using a camera or webcam. The system continuously captures frames in real-time. These images serve as the input for further processing. Proper lighting and camera positioning are important to ensure clear image quality.

### *B. Face Detection*

Once the image is captured, the system detects the presence of a human face in the frame. Face detection is performed using algorithms such as Haar Cascade or Histogram of Oriented Gradients (HOG). The system identifies the region of interest (ROI) where the face is located and ignores the background. This step is crucial to reduce unnecessary data processing.

### *C. Pre-processing*

After detecting the face, the image is pre-processed to improve quality and consistency. Pre-processing steps include resizing the image, converting it to grayscale or RGB format, noise reduction, and normalization. These steps help improve the accuracy of the recognition system.

### *D. Feature Extraction*

In this step, important facial features are extracted from the detected face. The system uses machine learning or deep learning models to convert the face into a numerical representation called a feature vector or embedding. These features include distances between facial landmarks such as eyes, nose, and mouth.

*E. Face Encoding*

The extracted features are converted into a fixed-length numerical encoding. This encoding uniquely represents a person's face. These encodings are stored in a database during the training phase and used later for comparison during authentication.

*F. Database Creation*

A database is created to store facial encodings along with user identity information. Multiple images of each person can be stored to improve accuracy. The database acts as a reference for recognizing authorized users.

*G. Face Recognition (Matching)*

In this stage, the system compares the encoding of the detected face with the stored encodings in the database. A similarity measure or distance metric (such as Euclidean distance) is used to determine if there is a match. If the similarity is within a predefined threshold, the face is recognized.

*H. Authentication Decision*

Based on the matching result, the system makes a decision:

- If a match is found → Access is granted
- If no match is found → Access is denied

This step ensures that only authorized users can access the system.

*I. System Implementation*

The system is implemented using Python programming language with libraries such as OpenCV for image processing and face_recognition for facial feature extraction. The system operates in real-time and provides quick responses.

*J. Testing and Validation*

Finally, the system is tested under different conditions such as varying lighting, angles, and facial expressions. Performance metrics like accuracy, precision, and response time are evaluated to ensure system reliability.

## VI. TOOLS AND TECHNOLOGIES

*1)* Programming Language: Python
*2)* Libraries: OpenCV, face_recognition, NumPy
*3)* Hardware: Webcam, Computer
*4)* Software: Arduino / VS Code

## VII. RESULTS AND ANALYSIS

The system achieves high accuracy under controlled conditions. Performance may decrease in poor lighting or with facial obstructions. The system shows fast response time and reliable recognition for registered users. The Facial Authentication System was tested under various conditions to evaluate its performance, accuracy, and reliability. The system was implemented using real-time video input through a webcam and tested with multiple users stored in the database.

## VIII. CONCLUSION

The Facial Authentication System presented in this research provides a modern, secure, and efficient solution for identity verification using biometric technology. Unlike traditional authentication methods such as passwords and ID cards, the proposed system utilizes unique facial features, making it more reliable and difficult to manipulate. In conclusion, the Facial Authentication System proves to be a promising and user-friendly approach for enhancing security in modern digital environments. With further improvements such as the use of advanced deep learning models, liveness detection, and cloud integration, the system can achieve even higher accuracy, scalability, and robustness in the future.

## IX. FUTURE SCOPE

The Facial Authentication System has significant potential for further development and improvement with the advancement of technology. Although the current system performs efficiently, there are several areas where enhancements can be made to increase accuracy, security, and usability.

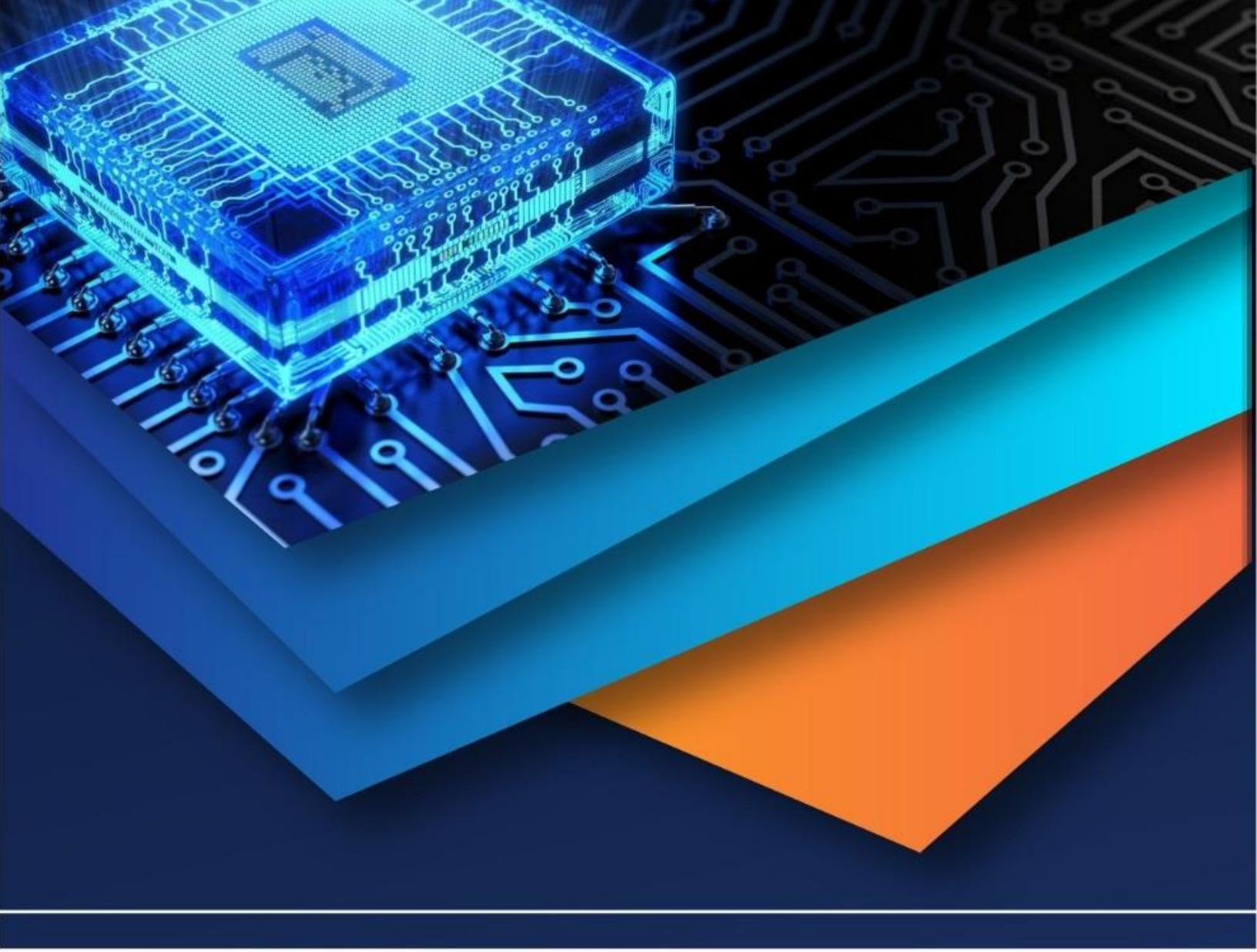
©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

In the future, the system can be improved by integrating advanced deep learning models such as Convolutional Neural Networks (CNNs) to achieve higher recognition accuracy even under challenging conditions like low lighting, different facial expressions, and varying angles. In conclusion, with continuous advancements in artificial intelligence and machine learning, the Facial Authentication System can evolve into a highly secure, scalable, and intelligent solution for modern authentication needs.

## REFERENCES

[1] Schroff, F., Kalenichenko, D., & Philbin, J., "FaceNet: A Unified Embedding for Face Recognition and Clustering," IEEE Conference on Computer Vision and Pattern Recognition, 2015.
[2] Viola, P., & Jones, M., "Rapid Object Detection using a Boosted Cascade of Simple Features," IEEE Conference on Computer Vision and Pattern Recognition, 2001.
[3] Zhang, K., Zhang, Z., Li, Z., & Qiao, Y., "Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks," IEEE Signal Processing Letters, 2016.
[4] Goodfellow, I., Bengio, Y., & Courville, A., Deep Learning, MIT Press, 2016.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)