International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Biometric Identification System using Computer Vision Technology for Automated Attendance Management

Abhishek Jaykumar Pal, Tushar Krishnachander Gupta, Vadlamudi Kalyan

B.Tech AIML, 4th Year, Sandip University, Nashik, Maharashtra, India

Guide: **Mr. Ayush Pandey**

https://doi.org/10.55041/ijsmt.v2i5.068

Cite this Article: Pal, A. J., Gupta, T. K. & Kalyan, V. (2026). Biometric Identification System using Computer Vision Technology for Automated Attendance Management. International Journal of Science, Strategic Management and Technology, *02*(05). https://doi.org/10.55041/ijsmt.v2i5.068

ABSTRACT

Accurate and efficient attendance management remains a significant challenge in educational institutions due to issues such as proxy attendance, manual errors, and time inefficiency. This paper proposes a multi-layer biometric attendance system based on computer vision techniques to address these limitations. The proposed system integrates face recognition as the primary identification method, enhanced with facial landmark validation, iris region localization, and basic anti-spoofing mechanisms to improve robustness, security, and accuracy.

The system is implemented using Python-based computer vision frameworks and operates on real-time video input for automated attendance marking. Facial embeddings are generated and matched against a structured database, while landmark-based geometric validation and iris region analysis act as additional verification layers. Furthermore, anti-spoofing measures such as live face verification (e.g., blink detection or facial movement analysis) are incorporated to prevent unauthorized access using photos or videos.

The system was evaluated on a dataset consisting of 50 users with over 200 facial samples, achieving an accuracy of 97.2%, with an average recognition time of 1–3 seconds per individual. Comparative analysis demonstrates that the proposed hybrid approach outperforms conventional single-modal face recognition systems in terms of reliability, security, and performance under varying environmental conditions.

The proposed solution is scalable, secure, and cost-effective, as it does not require specialized hardware, making it suitable for real-world deployment in educational and organizational environments. Future enhancements may include advanced deep learning-based anti-spoofing and encrypted cloud- based data management.

Keywords: Biometric Identification, Face Recognition, Computer Vision, Facial Landmarks, Iris Localization, Anti-Spoofing, Attendance Management

1.INTRODUCTION

In recent years, biometric identification systems have gained significant importance in the fields of security, authentication, and automation. These systems utilize unique physiological characteristics such as facial features, fingerprints, and iris patterns to identify individuals accurately. Among these, face recognition has emerged as one of the most widely adopted techniques due to its contactless nature, ease of implementation, and compatibility with standard imaging devices.

However, traditional attendance management systems used in educational institutions and organizations are still largely manual. These systems are time- consuming, prone to human errors, and vulnerable to proxy attendance and inaccurate

record keeping. Although face recognition-based attendance systems provide an automated alternative, they suffer from several limitations, including sensitivity to lighting conditions, pose variations, facial expressions, and partial occlusion. These factors often lead to false acceptance and false rejection, thereby reducing system reliability in real- world environments.

Recent research has attempted to address these limitations using deep learning- based face recognition models and hybrid biometric approaches. While such methods improve accuracy, most existing systems rely on a single biometric modality or require specialized hardware, such as dedicated iris scanners, which increases implementation cost and limits practical deployment. Furthermore, many existing systems lack anti-spoofing mechanisms, making them vulnerable to attacks using printed images or video playback.

To overcome these challenges, this paper proposes a multi-layer biometric attendance system using computer vision techniques that integrates face recognition with facial landmark validation, iris region localization, and lightweight anti-spoofing mechanisms.

Unlike conventional approaches, the proposed system is designed to operate using a standard webcam, eliminating the need for specialized hardware while maintaining high accuracy and security.

The system follows a multi-layer verification framework, where face recognition serves as the primary identification method, while facial landmark analysis validates geometric consistency and iris region localization provides an additional verification layer. Moreover, anti-spoofing techniques such as live face verification (e.g., blink detection or facial movement analysis) are incorporated to enhance system security and prevent unauthorized access.

The key contributions of this work are summarized as follows:

- Development of a multi-layer biometric verification framework combining face recognition, facial landmarks, and iris regionanalysis
- Integration of lightweight anti-spoofing mechanisms to improve system security against spoofin attacks
- Real-time implementation with an average recognition time of 1–3 seconds usinstandar hardware
- A cost-effective and scalable solution that does not require specialized biometricdevices
- Improved robustness under real-world conditions, including lighting variations and multi-user scenarios

The proposed system operates in real time, automates attendance marking, prevents duplicate entries, and ensures secure data management. By combining multiple verification layers with anti- spoofing capabilities, the system provides a practical, reliable, and secure solution for modern attendance management, addressing the limitations of existing single-modal and hardware-dependent approaches.

2.LITERATURE REVIEW

Biometric-based attendance systems have been widely explored as an effective alternative to traditional manual methods. Early approaches utilized technologies such as RFID cards and fingerprint recognition. RFID-based systems improve automation but depend on physical cards, which can be lost or misused, while fingerprint-based systems raise hygiene concerns and require direct contact [1].

Face recognition has emerged as a widely adopted contactless biometric solution for attendance management. Traditional techniques such as Principal Component Analysis (PCA) using Eigenfaces [2], Linear Discriminant Analysis (LDA) [3], and Local Binary Pattern Histogram (LBPH) [4] have been used for feature extraction and classification. Although these methods achieve moderate accuracy, they are highly sensitive to variations in lighting conditions, pose, and facial expressions.

Recent advancements in deep learning, particularly Convolutional Neural Networks (CNNs), have significantly improved face recognition performance. Studies such as DeepFace [5] and FaceNet [6] demonstrate that deep learning-based models can achieve high accuracy under controlled conditions. However, these approaches primarily rely on a single biometric modality, making them vulnerable to false acceptance, false rejection, and spoofing attacks.

To address security concerns, researchers have introduced face anti-spoofing techniques, also known as liveness detection. These methods aim to distinguish between real human faces and fake inputs such as printed images,videos, or

masks. Common approaches include texture-based analysis, motion- based detection (e.g., eye blinking or head movement), and deep learning- based classification models [7]. While these techniques improve system security, many implementations increase computational complexity or require additional hardware.

In addition to anti-spoofing, computer vision frameworks such as OpenCV and MediaPipe have enabled more detailed analysis of facial features through landmark detection. Facial landmark techniques identify key facial points such as eyes, nose, and mouth, which can be used for geometric validation and improved recognition robustness. Similarly, iris-based biometric systems are known for their high accuracy due to the uniqueness of iris patterns [8]. However, most iris recognition systems require specialized hardware, limiting their practical applicability.

Recent research trends focus on hybrid biometric systems that combine multiple modalities to improve accuracy, reliability, and security. While such systems demonstrate improved performance, many existing approaches increase system complexity or rely on expensive hardware setups, making them less suitable for real-time deployment in resource-constrained environments [9].

Therefore, there exists a need for a lightweight, cost-effective, and secure hybrid biometric system that can operate in real time using standard hardware while resisting spoofing attacks. The proposed system addresses this gap by integrating face recognition with facial landmark validation, iris region localization, and lightweight anti- spoofing mechanisms into a unified multi-layer framework for automated attendance management.

3.PROPOSED METHODOLOGY

3.1System Overview

The proposed system is a multi-layer biometric attendance framework designed for accurate, secure, and real- time attendance management using computer vision. Unlike conventional single-modal systems that rely solely on face recognition, the proposed approach integrates face recognition, Insight-based facial landmark validation (MediaPipe Face Mesh), iris region localization, and lightweight anti-spoofing mechanisms.

A key advantage of the system is that it operates using a standard webcam, eliminating the need for specialized biometric hardware while maintaining high accuracy and security. A user- friendly interface is incorporated to facilitate efficient interaction between the administrator and the system.

3.2System Architecture

The system follows a modular, multi- stage pipeline comprising:

1. User Interface Module
2. Face Detection Module
3. Face Recognition Module
4. Facial Landmark (Insight) Analysis Module
5. Iris Region Localization Module
6. Anti-Spoofing Module
7. Hybrid Verification Engine
8. Attendance Management Module
9. Database Module

Each module performs a dedicated function, contributing to overall system accuracy, robustness, and security.

3.3User Interface Module

An interactive interface is developed using Streamlit to enable:

- Student registration
- Image/data capture
- Model training

Real-time attendance monitoring

- Report viewing and export

The interface is designed for ease of use and requires minimal technical expertise.

3.4 Face Detection Module

Real-time video frames are captured via a webcam. Faces are detected using MediaPipe Face Detection (or OpenCV-based detectors), providing bounding boxes for each detected face. Detected regions are aligned and normalized before further processing to ensure consistency across varying conditions.

3.5 Face Recognition Module

Facial features are converted into compact numerical representations (embeddings) using a deep learning- based model (e.g., *face_recognition* library).

Identification is performed by comparing embeddings with stored vectors using a Euclidean distance metric with a predefined threshold. This enables fast and accurate matching in real time.

3.6 Facial Landmark (Insight) Analysis Module

Facial landmark extraction is performed using the MediaPipe Face Mesh (Insight- based technique), which provides up to 468 key points across the face.

These landmarks are used to:

- Validate facial geometry and alignment
- Check pose consistency
- Support liveness cues (micro- movements)

This layer improves robustness against variations in pose, expression, and partial occlusion.

3.7 Iris Region Localization Module

The system performs iris region localization using eye-region landmarks obtained from the Face Mesh model. Landmark indices corresponding to eye contours are used to isolate the iris region.

The localized iris serves as an auxiliary verification cue, strengthening identity confirmation without requiring infrared sensors or dedicated iris scanners. This design ensures cost-effectiveness and deployability on standard hardware.

3.8 Anti-Spoofing Module

To enhance security, a lightweight anti- spoofing mechanism is incorporated using temporal and landmark-based cues derived from the Insight model. The system analyzes:

- Eye blink patterns
- Subtle facial movements (e.g., head motion)

These signals help distinguish live faces from spoofing attempts such as printed photos or video playback, thereby reducing unauthorized access.

3.9 Hybrid Verification Engine

A multi-layerdecisionstrategy aggregates outputs from all modules:

- Primary Layer: Face Recognition (embedding similarity)
- SecondaryLayer:Landmark Validation (geometric consistency)
- Tertiary Layer:IrisRegion Localization
- SecurityLayer:Anti-Spoofing (liveness)

A final confidence decision is computed by combining these layers, significantly improving accuracy, robustness, and resistance to spoofing compared to single-modal approaches.

3.10 Attendance Management Module Upon successful verification, attendance is automatically recorded with date and timestamp. The system enforces a one- entry-per-user-per-day policy to prevent duplicates and ensures consistent record keeping.