Facial Recognition Based Attendance System With Anti Spoofing Method

[1] Dr. N. Manjunatha,[2] Johnson J.W, [3] Pavan S.S, [4] Kaushik. T, [5] Sai Pavan R.S,
[1]Assistant Professor ,[2]Student, [3]Student, [4]Student, [5]Student, [1]
CSE(AI-ML)
,
[1]R L Jalappa Institute Of Technology , Bengaluru, India
[1]manjunatha22@gmail.com, [2]johnsonjoseph3332@gmail.com, [3]sspavan25@gmail.com,
[4]kaushikpurothith@gmail.com, [5]r9353514864@gmail.com

Abstract— Attendance monitoring remains a fundamental yet inefficient task in educational institutions, where manual roll calls and basic electronic systems continue to dominate. These approaches introduce time overhead, administrative burden, and susceptibility to proxy attendance. Although biometric solutions such as fingerprint and RFID systems offer partial automation, they suffer from hygiene concerns, hardware maintenance issues, and scalability limitations. This paper presents the design, implementation, and evaluation of a deployable facial- recognition-based attendance system optimized for classroom environments. The system integrates Haar Cascade face detection with Local Binary Pattern Histogram (LBPH) recognition and incorporates a multi-stage liveness verification pipeline combining Eye Aspect Ratio (EAR)-based blink detection with a lightweight CNN–LSTM temporal model. Attendance is recorded only when both identity recognition and liveness verification exceed pre- defined confidence thresholds. Extensive experiments conducted under realistic classroom conditions demonstrate recognition accuracy between 92% and 97%, liveness detection rates exceeding 90%, and real-time performance of 8–10 frames per second on CPU-only hardware. The proposed solution achieves a practical balance between ro- business, spoof resistance, and computational efficiency, making it suitable for deployment in resource-constrained academic institutions.

Index Terms— Face recognition, automated attendance, liveness detection, anti-spoofing, classroom analytics, applied computer vision.

Introduction

Attendance is more than a formality in educational institutions, it directly affects academic evaluation, regulatory compliance, and how student performance is tracked. Yet, many institutions still depend on manual or partially automated attendance systems that are slow, disruptive, and easy to exploit. Traditional roll calls break the flow of teaching, waste classroom time, and often result in recording errors or proxy attendance.

To overcome these issues, token-based systems such as RFID cards and barcode scanners have been adopted. While these methods reduce manual effort, they introduce new problems. Students can easily share cards, and in- situations must deal with ongoing costs related to card issuance, replacements, and hardware upkeep. Fingerprint- based biometric systems improve identity verification but raise hygiene concerns and tend to lose accuracy over time due to sensor wear and environmental factors.

Facial recognition has emerged as a practical, contactless alternative that can operate in the background using standard cameras. It improves user convenience and removes the need for physical interaction. However, basic face recognition systems are vulnerable to spoofing attacks, such as using printed photographs or replaying videos on mobile screens. In classroom settings with minimal supervision, these low-effort attacks are both realistic and difficult to prevent.

Although recent deep learning models have achieved impressive accuracy in face recognition and liveness detection, they often depend on powerful GPUs, massive datasets, and complex system setups. These requirements make them unsuitable for routine deployment in most educational institutions. This work therefore focuses on a system-level design that prioritizes practicality—ensuring the solution is computationally efficient, easy to main- train, and feasible to deploy in real-world academic environments.

Problem Statement

The core problem addressed in this work is the development of an automated attendance system that operates reliably in classroom environments while resisting common spoofing attacks. The system must satisfy several constraints: real-time operation on CPU-based hardware, robustness to moderate illumination and pose variations, resistance to presentation attacks, and ease of deployment without specialized biometric hardware.

Formally, given a continuous video stream captured from a classroom camera, the system must detect faces, recognize enrolled students, verify liveness, and record attendance events in a secure and auditable manner. These tasks must be performed under realistic constraints such as limited computational resources, unconstrained student behavior, and variable environmental conditions.

System Architecture

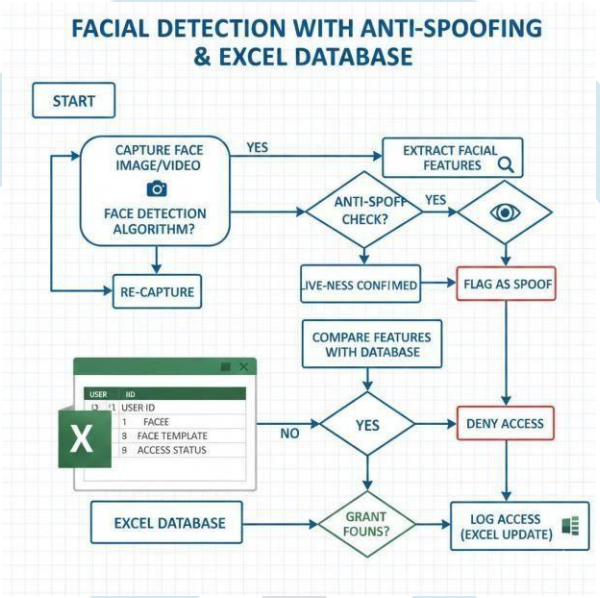

Figure 1: System Flow Diagram

The proposed system follows modular pipeline architecture. A live video stream is captured using an off-the-shelf HD webcam. Each frame undergoes face detection, recognition, and liveness verification before attendance is logged.

The modular design allows independent optimization of each component and facilitates future upgrades without redesigning the entire system.

Methodology

Video Acquisition and Preprocessing

The video acquisition module captures frames at a resolution of 720p. Frames are converted to grayscale and normalized to reduce sensitivity to illumination variations. Histogram equalization is optionally applied to enhance contrast in low-light conditions.

Face Detection

Face detection is implemented using the Viola–Jones Haar Cascade framework. The detector employs a cascade

of boosted classifiers trained on Haar-like features, enabling rapid rejection of non-face regions while maintaining acceptable detection accuracy for frontal faces.

Face Recognition Using LBPH

Local Binary Pattern Histogram (LBPH) is employed for face recognition due to its robustness to illumination changes and low computational overhead. Each detected face is resized to a fixed resolution and divided into local regions. Binary patterns are computed for each pixel neighborhood and aggregated into histograms.

During enrollment, multiple samples per student are captured under varying conditions. During recognition, the histogram of the detected face is compared against stored templates using a distance metric, and the identity with the minimum distance is selected.

Blink-Based Liveness Detection

Blink detection is performed using the Eye Aspect Ratio (EAR), defined as:

$$\text{EAR} = \frac{\|p_2 - p_6\| + \|p_3 - p_5\|}{2\|p_1 - p_4\|}$$

Temporal variations in EAR values are analyzed over a sliding window to detect natural blinking behavior.

CNN–LSTM Temporal Liveness Analysis

To counter replay attacks, a compact CNN–LSTM model is employed. The CNN extracts spatial texture features from each frame, while the LSTM captures temporal dependencies across a short frame sequence. The model outputs a liveness probability used in the final decision stage.

Algorithm Description

1. Capture video frame from webcam.
2. Detect faces using Haar Cascade.
3. For each detected face:
   (a) Extract LBPH features and perform recognition.
   (b) Compute EAR values and detect blinks.
   (c) Extract temporal features and evaluate CNN–LSTM liveness score.
   (d) Fuse recognition and liveness scores.
   (e) Log attendance if thresholds are satisfied.

Experimental Setup

Experiments were conducted in classroom-like environments using a desktop system equipped with an Intel Core i5/i7 CPU, 16 GB RAM, and a 720p webcam. No GPU acceleration was used.

The dataset included genuine student sessions, printed photo spoof attempts, and video replay attacks displayed on mobile devices.

Results and Analysis

Recognition Performance

The face recognition module achieved accuracy ranging from 92% to 97%, depending on lighting conditions and seating positions.

Liveness Detection Performance

Static photo attacks were effectively rejected by blink-based detection, while replay attacks were primarily detected by the CNN–LSTM model.

Table 1: Performance Summary

Metric	Min	Max	Avg
Recognition Accuracy (%)	92	97	94.5
Liveness Accuracy (%)	90	95	92.3
Throughput (FPS)	8	10	9

Computational Complexity Analysis

Haar Cascade detection operates in approximately linear time with respect to the number of pixels. LBPH feature extraction scales linearly with face region size. The CNN–LSTM model introduces additional overhead but remains feasible for real-time operation due to its shallow architecture and short temporal windows.

Security and Privacy Considerations

Biometric data storage introduces privacy risks. The proposed system stores only feature representations rather than raw images and operates entirely on local infrastructure, avoiding cloud-based data transmission.

Limitations

The system may experience reduced accuracy under extreme lighting conditions, heavy occlusions, or highly sophisticated spoofing attacks. The use of LBPH limits performance under large pose variations.

Future Work

Future enhancements include adaptive thresholding, integration of depth-based cues, incremental learning, and improved user interfaces for administrative control.

Conclusion

This paper presented a deployable facial-recognition-based attendance system with multi-stage liveness verifica- tion optimized for classroom environments. The system demonstrates that a hybrid approach combining classical computer vision and lightweight deep learning can achieve reliable performance on commodity hardware.

References

1. P. Viola and M. Jones, “Rapid object detection using a boosted cascade of simple features,” Proc. IEEE CVPR, 2001.
2. S. Z. Li and A. K. Jain, Handbook of Face Recognition. Springer, 2011.
3. T. Soukupová and J. Cˇ ech, “Real-time eye blink detection using facial landmarks,” Proc. CVWW, 2016.
4. Z. Wu et al., “Video-based face anti-spoofing using CNN–LSTM models,” IEEE Access, vol. 7, pp. 24821– 248