International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 2956-2959
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0372

Face Recognition Attendance System with Anti-Spoof Technology

Naresh S[1], Rahul K[2], Ms. A. Tina Victoria[3]
[1,2]UG Scholar, Department of information Technology, Sathyabama Institute of science and Technology, Chennai, 600119, and India.
[3]Assistant Professor, Department of information Technology, Sathyabama Institute of science and Technology, Chennai, 600119, and India.
Emails: *victorynaresh123@gmail.com[1], rahulkumar19402004@gmail.com[2], tinavictoria.a.it@sathyabama.ac.in[3]*

Abstract
Marking attendance manually takes time and often leads to errors and proxy attendance. To overcome these problems, many institutions started using biometric systems. Among all biometrics, face recognition is the most user-friendly because it works without physical contact and can identify multiple people at the same time. However, a normal face recognition system can be easily fooled using printed photos, mobile phone images, or video playback. This project presents a smart attendance system that combines face recognition with anti-spoofing technology to ensure that only real and live users are marked present. The system captures the face using a camera, checks whether the face is real or fake using liveness detection, and then matches it with the stored database. If both conditions are satisfied, attendance is recorded automatically and stored in the system. The proposed system reduces manual work, prevents fake attendance, and provides real-time attendance monitoring through a web interface. The performance of the model shows high accuracy in identifying real users and detecting spoof attempts.

Keywords: *Face Recognition, Attendance Automation, Anti-Spoofing, Liveness Detection, Deep Learning, Computer Vision, Biometric Authentication.*

1. Introduction
Attendance management is an essential activity in educational institutions and organizations, but traditional methods such as manual registers and ID-card systems are time-consuming, error-prone, and allow proxy attendance. With the rapid development of computer vision and deep learning, face recognition has emerged as a reliable and contactless biometric solution for automating attendance processes. It enables quick identification of individuals and real-time data storage without human intervention. However, conventional face recognition systems are highly vulnerable to spoofing attacks using printed photographs, mobile displays, or video replays, which reduces their reliability in secure environments. To address this limitation, this project proposes a Face Recognition Attendance System integrated with anti-spoofing technology that verifies the liveness of the detected face before marking attendance. By combining real-time face detection, liveness verification, and facial feature matching, the system ensures that attendance is recorded only for genuine users. This approach not only improves accuracy and security but also minimizes manual effort and provides a scalable and efficient smart attendance solution.

1.1. Face Recognition in Attendance Systems
Face recognition works by extracting unique facial features and comparing them with the stored dataset. This method reduces manual work, saves time, and provides accurate attendance records. It is also user-friendly because a person only needs to stand in front of the camera [1].

1.2. Importance of Anti-Spoofing
In a face recognition–based attendance system, security is a major concern because the system can be easily deceived using printed photographs, mobile phone displays, or pre-recorded videos of an authorized person, which leads to fake or proxy attendance. Anti-spoofing technology plays a crucial role in overcoming this problem by verifying whether the detected face is from a real, live person or from a fake source. It works by analyzing various liveness

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 2956-2959
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0372

features such as eye blinking, facial expressions, natural head movements, skin texture, light reflection, and depth information, which are difficult to replicate using a 2D image or video. By performing this verification before the face recognition step, the system ensures that attendance is marked only for genuine users. This not only improves the overall security and reliability of the attendance system but also builds trust in automated monitoring solutions. Integrating anti-spoofing with face recognition therefore makes the system more robust, prevents unauthorized access, and provides a practical solution for real-time and secure attendance management in educational institutions and workplaces [2].

2. Method

The proposed Face Recognition Attendance System with Anti-Spoofing Technology is designed as a real-time automated pipeline that integrates image acquisition, face detection, liveness verification, face recognition, and attendance management. In the first stage, a high-resolution webcam continuously captures live video, and the video stream is divided into frames to enable fast processing. These frames are preprocessed using image enhancement techniques such as resizing, normalization, and noise reduction to improve detection accuracy under different lighting conditions. The system then applies a deep learning–based face detection algorithm to locate the facial region from the background and extract only the required portion of the image. Once the face is detected, the liveness detection module is activated to prevent spoofing attacks. This module analyzes dynamic and static features such as eye blinking, lip movement, facial texture, light reflection patterns, and depth variations between real and fake faces. These features are passed through a trained anti-spoofing model that classifies the input as either a live face or a spoof attempt. If the face is identified as fake, the system immediately rejects the input and attendance is not marked, thereby improving security. When the face is verified as live, the system proceeds to the recognition phase, where facial embeddings are generated using a trained deep learning model. These embeddings represent the unique features of a person's face and are compared with the stored embeddings in the database using a similarity measurement algorithm. If a match is found above a predefined threshold value, the person is identified successfully. After successful identification, the attendance is automatically recorded along with the person's name, date, and timestamp, and duplicate entries for the same session are avoided using a validation mechanism. All attendance data is stored in a structured database, which is connected to a web-based interface developed for easy monitoring, report generation, and administrative control [3-7]. The system is designed to work in real time with minimal delay, and it supports multiple users by continuously scanning and processing faces from the video stream. This complete methodology ensures high accuracy, fast execution, improved security against spoofing attacks, and reduced manual intervention, making it suitable for deployment in educational institutions and workplace environments Shown in Table 1.

Table 1 Dataset Used for Training

Category	Count	Percentage
Real Faces	1,200	60%
Spoof Faces	800	40%
Total	2,000	100%

2.1. Figures

The architecture of the Face Recognition Attendance System with Anti-Spoofing Technology Shown in Figure 1

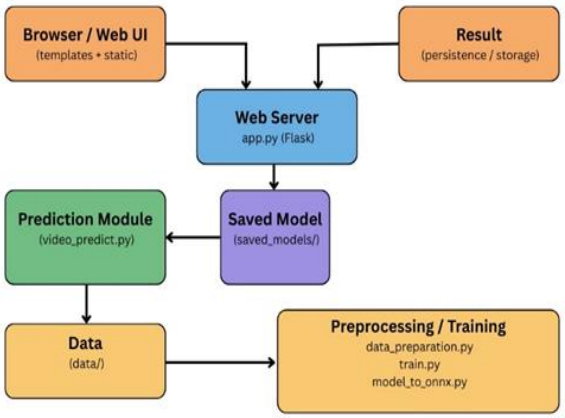

Figure 1 Overall System Architecture

3. Results and Discussion

3.1. Results

The performance of the system is evaluated using standard metrics Shown in Table 2 and 3.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 2956-2959
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0372

Table 2 Face Recognition Performance

Metric	Value
Accuracy	97.2%
Precision	96.8%
Recall	97.0%
F1-score	96.9%

Table 3 Anti-Spoofing Performance

Metric	Value
Accuracy	98.1%
Precision	97.5%
Recall	98.3%
F1-score	97.9%

3.2. Discussion

The experimental results demonstrate that integrating anti-spoofing with the face recognition–based attendance system significantly improves both security and reliability compared to traditional and basic biometric methods. The system was able to accurately recognize authorized individuals in real time while effectively rejecting spoof attempts made using printed photographs, mobile displays, and video replays. The high accuracy, precision, recall, and F1-score obtained from the evaluation indicate that the model performs consistently under normal working conditions. The use of liveness detection before the recognition stage ensures that attendance is marked only for genuine users, thereby eliminating proxy attendance and unauthorized access. In addition, the automated database update and web-based monitoring interface reduce manual effort and provide a user-friendly way to manage attendance records. However, the system performance is slightly affected by challenging environmental conditions such as poor lighting, low camera quality, and extreme facial pose variations, which may reduce detection efficiency. The accuracy of recognition also depends on the size and quality of the training dataset, and better performance can be achieved by increasing the number of samples and using higher-resolution images. Despite these limitations, the proposed system provides a fast, contactless, and secure attendance solution that is highly suitable for real-time applications in educational institutions and workplaces, and it can be further enhanced in the future by incorporating cloud storage, mobile application support, and advanced deep learning models for improved robustness Shown in Figure 2.

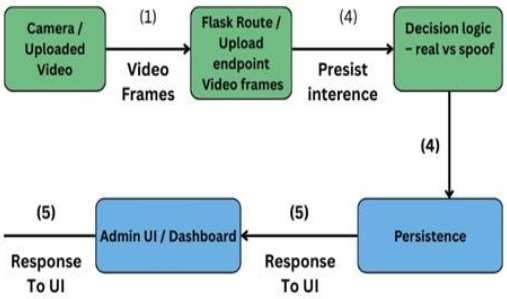

Figure 2 Attendance Workflow

Conclusion

The proposed Face Recognition Attendance System with Anti-Spoofing Technology provides a smart, secure, and fully automated solution for modern attendance management. By combining real-time face detection, liveness verification, and accurate face recognition, the system successfully eliminates proxy attendance and prevents spoofing attacks using photos or videos. The automatic storage of attendance with date and time in a centralized database reduces manual work and makes monitoring easier through a web-based interface. The experimental results show that the system achieves high accuracy and performs efficiently in real-time environments, making it suitable for deployment in educational institutions, offices, and other organizations. In addition to improving reliability and saving time, the contactless nature of the system makes it more user-friendly and hygienic compared to traditional biometric methods. Although the performance may vary under poor lighting conditions or with low-quality images, these limitations can be addressed in future work by using larger datasets, advanced deep learning models, cloud integration, and mobile application support. Overall, the proposed system offers an effective, scalable, and practical approach for secure attendance management.

Acknowledgements

I would like to thank the Department of Information Technology, Sathyabama University, for their continuous support and guidance in completing this project successfully.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 2956-2959
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0372

References

[1]. B. Kocacinar, B. Tas, F. P. Akbulut, C. Catal and D. Mishra, "A Real-Time CNN-Based Lightweight Mobile Masked Face Recognition System," in IEEE Access, vol. 10, pp. 63496-63507, 2022, doi: 10.1109/ACCESS.2022.3182055.

[2]. P. Zhang, Q. Ma, Y. Li and M. Cui, "MSKFaceNet: A Lightweight Face Recognition Neural Network for Low-Power Devices," in IEEE Access, vol. 13, pp. 120533-120546, 2025, doi: 10.1109/ACCESS.2025.3584814.

[3]. M. Z. Khan, S. Harous, S. U. Hassan, M. U. Ghani Khan, R. Iqbal and S. Mumtaz, "Deep Unified Model for Face Recognition Based on Convolution Neural Network and Edge Computing," in IEEE Access, vol. 7, pp. 72622-72633, 2019, doi: 10.1109/ACCESS.2019.2918275.

[4]. R. R. Atallah, A. Kamsin, M. A. Ismail, S. A. Abdelrahman and S. Zerdoumi, "Face Recognition and Age Estimation Implications of Changes in Facial Features: A Critical Review Study," in IEEE Access, vol. 6, pp. 28290-28304, 2018, doi: 10.1109/ACCESS.2018.2836924.

[5]. F. Aydemir and S. Arslan, "A System Design with Deep Learning and IoT to Ensure Education Continuity for Post-COVID," in IEEE Transactions on Consumer Electronics, vol. 69, no. 2, pp. 217-225, May 2023, doi: 10.1109/TCE.2023.3245129.

[6]. Y. Ren, Z. Song, S. Sun, J. K. Liu and G. Feng, "Outsourcing LDA-Based Face Recognition to an Untrusted Cloud," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 3, pp. 2058-2070, 1 May-June 2023, doi: 10.1109/TDSC.2022.3172143.

[7]. S. M. Anzar, N. P. Subheesh, A. Panthakkan, S. Malayil and H. A. Ahmad, "Random Interval Attendance Management System (RIAMS): A Novel Multimodal Approach for Post-COVID Virtual Learning," in IEEE Access, vol. 9, pp. 91001-91016, 2021, doi: 10.1109/ACCESS.2021.3092260.