Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 10s (2025)

Hybrid Deep Learning based Smart Attendance System with Robust Anti Spoofing Mechanism

Bisweswar Thakur[1]
[1]PG Student, School of Computational Sciences, Faculty of Science and Technology, JSPM University Pune,
Pune, Maharashtra, India

Rahul Chakre[2]
[2]Sr. Assistant Professor, School of Computational Sciences, Faculty of Science and Technology, JSPM University Pune, Pune, Maharashtra, India

Article History:
Received: 14-01-2025
Revised: 16-02-2025
Accepted: 05-03-2025

Abstract: This paper introduces an innovative smart attendance system that employs deep learning-based face recognition, seamlessly integrated with advanced anti-spoofing techniques, to deliver secure and dependable attendance management for both educational and corporate settings. The system leverages a refined hybrid algorithm, optimized through parameter tuning, to enhance recognition accuracy and effectively mitigate fraudulent attempts. Evaluated on standard benchmark datasets (indexed in SCIE and Scopus), the system demonstrates superior real-time performance. Experimental results reveal high accuracy, fast processing, and strong resilience against spoofing attacks. As face recognition becomes an increasingly prominent biometric authentication method in security-critical environments, it remains vulnerable to spoofing threats such as printed photographs and video replay attacks, a challenge this work directly addresses. This research proposes a Smart Attendance System enhanced with an anti-spoofing module combining convolutional neural networks (CNN), temporal modelling using LSTM, motion and blink detection, and robust face recognition via FaceNet and SVM. We employ datasets including CASIA-FASD to construct and fine-tune our model. Experimental evaluation confirms our system achieves high accuracy with significant spoof-resistance. This integrated approach ensures reliability for real-time applications like institutional attendance, banking security.

Keywords: *Face Recognition, Anti-Spoofing, Deep Learning, Smart Attendance, Modified Algorithm, Hybridized Algorithm, Parameter Tuning, Parameter Optimization, Benchmark Dataset, MobileNetV2, LSTM, Smart Attendance, Blink Detection, Motion Analysis.*

1. Introduction

Attendance management in classrooms and workplaces is a critical process that traditionally relies on manual or semi-automated methods. Recent advancements in deep learning have enabled the development of automated attendance systems that not only streamline this process but also significantly reduce errors and fraudulent practices such as proxy attendance. In this study, we introduce a smart attendance system based on deep learning-based face recognition integrated with advanced anti-spoofing techniques. By modifying and hybridizing existing algorithms and performing rigorous parameter tuning and optimization, our system ensures both high accuracy and security. Biometric-based authentication systems have seen significant advancements with face recognition at the forefront due to its non-intrusiveness and convenience. Despite improvements in face recognition accuracy, the challenge of spoofing attacks persists. To mitigate these vulnerabilities, integrating robust liveness detection and anti-spoofing mechanisms becomes crucial. The proposed work integrates multiple techniques like blink detection, motion analysis, CNN, and LSTM models to counteract spoofing attempts while ensuring reliable attendance marking. With rapid advancements in technology, it makes sense to leverage it effectively. Face recognition offers a reliable solution for attendance tracking, reducing the risk of fraud and errors that often occur with traditional methods. Implementing this technology in universities ensures accuracy and efficiency. By selecting the right algorithm, institutions can optimize attendance tracking and minimize errors. This study reviews existing research to identify the most effective algorithm for face recognition and explores strategies to reduce inaccuracies in real-world applications.

2. Literature Review

Face recognition systems are increasingly used in security-sensitive applications, including smart attendance systems. However, traditional methods often fail to detect spoofing attacks, such as photo or video replays. Thus, anti-spoofing methods combining temporal, texture, and physiological cues have emerged. Recent advancements include UCDCN (Zhang et al., 2024), which uses central difference convolution and UNet++ fusion for efficient spoofing detection. Other CNN-based models such as CDCN, NAS-FAS, and FAS-BAS integrate depth supervision or multi-frame learning to enhance spoof-resistance. Traditional texture-based methods like LBP, HOG, and SURF were earlier utilized but failed under high-resolution or variant lighting. Time-based approaches, particularly those leveraging blinking or micro-movements, have shown promise for temporal modeling.

Mahmoud Ali *et al.* [1] introduced an innovative face recognition system that integrates Multi-task Cascaded Convolutional Neural Networks (MTCNN) for precise face detection, VGGFace for feature extraction, and Support Vector Machine (SVM) for efficient classification. The system demonstrates exceptional real-time performance in tracking multiple faces within a single frame, particularly excelling in attendance monitoring. The "VGGFace" model emerges as a standout performer, showcasing remarkable accuracy and achieving an impressive F-score of 95% when coupled with SVM. This underscores the model's effectiveness in recognizing facial identities, attributing its success to robust training on extensive datasets. The research highlights the potency of the VGGFace model, especially in collaboration with various classifiers, with SVM yielding notably high accuracy rates.

Bao-Thien Nguyen-Tat *et al.* [2] proposed a Face Recognition Attendance Management System (FRAMS) utilizes facial recognition technology to efficiently identify and record the presence of individuals. The system combines Haar Cascade, a cost-effective and user-friendly machine learning algorithm, with the processing power of the NVIDIA Jetson Nano to accurately detect and match faces in a database, minimizing manual intervention and reducing errors. The researchers emphasize the system's accessibility, scalability, and commitment to privacy, making it a transformative solution for attendance management in educational institutions, workplaces, and other settings. Nico Surantha *et al.* [3] presented a lightweight face recognition-based portable attendance system with liveness detection. Face recognition systems are vulnerable to face spoofing attacks, where an attacker can disguise themselves as an authorized individual. To address this, the proposed system implements a liveness detection step before the face recognition process. The goal is to develop a lightweight liveness detection method that can run on a Raspberry Pi device. The system uses the MobileNetV2 model trained with transfer learning for liveness detection, achieving high accuracy in detecting live subjects and various levels of spoofing attacks. The proposed attendance system has an average processing time below 0.6 seconds, making it suitable for portable deployment.

Edward Yose *et al.* [4] This paper presents the development of a portable smart attendance system using the Jetson Nano embedded system. The system aims to recognize individuals even when they are wearing a mask, without requiring them to remove it. It uses an innovative method that can accurately detect and recognize faces, even when partially obscured by masks. The system is designed to be fully autonomous, with minimum physical interaction required from students or employees. It captures facial images, performs face alignment, and compares them against a database to mark attendance. The system is intended to improve the performance, accuracy, and efficiency of attendance tracking, especially in light of the COVID-19 pandemic and the widespread use of face masks. S. Velasquez Caceres *et al.* [5] aimed to develop a facial recognition system for attendance taking in university classrooms in Peru. The system utilizes cameras and artificial intelligence based on machine learning to automate the attendance process and address the issues of delays and human errors associated with traditional manual methods. The project employs the VDI 2206 design methodology to establish requirements, conduct initial design, and develop electronic models for integration into the proposed system. The expected outcomes include a detailed electrical diagram, a flowchart of the facial recognition process, a programming model for accurate student identification, and an implementation model in a real-world environment. The proposed system aims to optimize and streamline the attendance taking process, enhance academic management, and contribute to an improved educational experience. Zhang et al. [6] proposed a CNN + RNN hybrid for face anti-spoofing using spatial and temporal features. Dataset: CASIA-FASD, Replay-Attack. George et al. [7] introduced deep pixel-wise supervision for face spoof detection. Achieved over 90% accuracy on CASIA-FASD. Liu et al. [8] used a dual-stream 3D CNN for depth and motion-based detection. Dataset: OULU-NPU. Bhattacharjee and Das [9] proposed blink detection using Eye Aspect Ratio (EAR) from dlib landmarks.

Tabulated Survey of Similar Works

Paper	Model Used	Dataset Used	Temporal Modelling	Accuracy (%)	Spoof Types Detected
Zhang et al. [10]	CNN + RNN	CASIA, Replay	Yes	89.2	Print, Replay, Cut Photos
George et al. [11]	Deep CNN	CASIA-FASD	No	90.1	Print, Video, Mask
Liu et al. [12]	Dual-stream 3D CNN	OULU-NPU	Yes	92.5	Photo, Replay, 3D Mask
Bhattacharjee and Das [13]	Blink Detection + EAR	Custom	Yes	82.3	Photo, Static Spoof

Advantages of Existing Systems:

- Good performance on static spoof detection (photo, video).
- End-to-end deep learning pipelines.
- Blink detection provides real-time physiological cues.

Disadvantages of Existing Systems:

- Limited robustness across diverse lighting and device conditions.
- Heavy reliance on large annotated video datasets.
- Lack of fusion of multiple liveness cues (motion + blink + CNN).

3. Objectives

Develop a modified face recognition algorithm that combines the strengths of multiple models. Implement a hybridized approach that integrates liveness detection with traditional face recognition. Perform extensive parameter tuning and optimization to improve recognition and spoof detection accuracy. Validate the system using standard benchmark datasets indexed in SCIE and Scopus. Deploy the system in a cloud environment (AWS) for scalable real-time operation. To develop a real-time face recognition-based attendance system. To integrate a lightweight yet accurate liveness detection mechanism using CNN and LSTM. To combine blink detection and motion analysis as secondary cues. To evaluate and validate the model performance against benchmark spoof datasets.

4. Methodology

The proposed methodology for a Classroom Smart Attendance System using Computer Vision (CV) and Deep Learning (DL) aims to create an automated, real-time, and accurate attendance system. This methodology addresses environmental variability, fairness, privacy, and computational efficiency, ensuring that it operates effectively on edge devices. The methodology can be broken down into several key steps, as outlined below:

4.1. Data Acquisition and Preprocessing

- **Data Collection:** Gather face images and videos from standard datasets (e.g., CASIA-FASD, as well as custom-collected data [10][11].
- **Preprocessing:** In data augmentation, to enhance model robustness, augmentation techniques are applied. This includes rotation and scaling for pose invariance, brightness adjustment to mimic various lighting conditions, flipping and cropping to simulate real-world variances in captured images. In labelling each face in the dataset is labelled with the corresponding student ID to create a supervised dataset. For automated labelling, existing tools or manual checks ensure accuracy in tagging each student's face.

4.3. Face Detection Algorithm

In face detection phase we have used MTCNN (Multi-Task Cascaded Convolutional Network). It is a deep learning-based face detector used to detect face landmarks. RetinaFace is a more advanced deep learning-based detector that performs pixel-wise face localization.

Step-by-Step Process

a) Capture live video stream from the webcam.
b) Convert the image to grayscale for faster processing.
c) Apply the MTCNN model to detect face bounding boxes [12].
d) Extract the region of interest (ROI) where the face is located.
e) Pass the extracted face to the face recognition model for identity verification.

4.4. Face Recognition Algorithm

A pretrained FaceNet model is used for face recognition. FaceNet generates a 128-dimensional feature vector for face embedding. ArcFace enhances intra-class compactness and inter-class separability, improving face recognition accuracy. For classification SVM(Support Vector Machine) are used. If the face matched with database then attendance store in the database, otherwise the face will be rejected. Figure1 shows the overall face recognition system architecture.

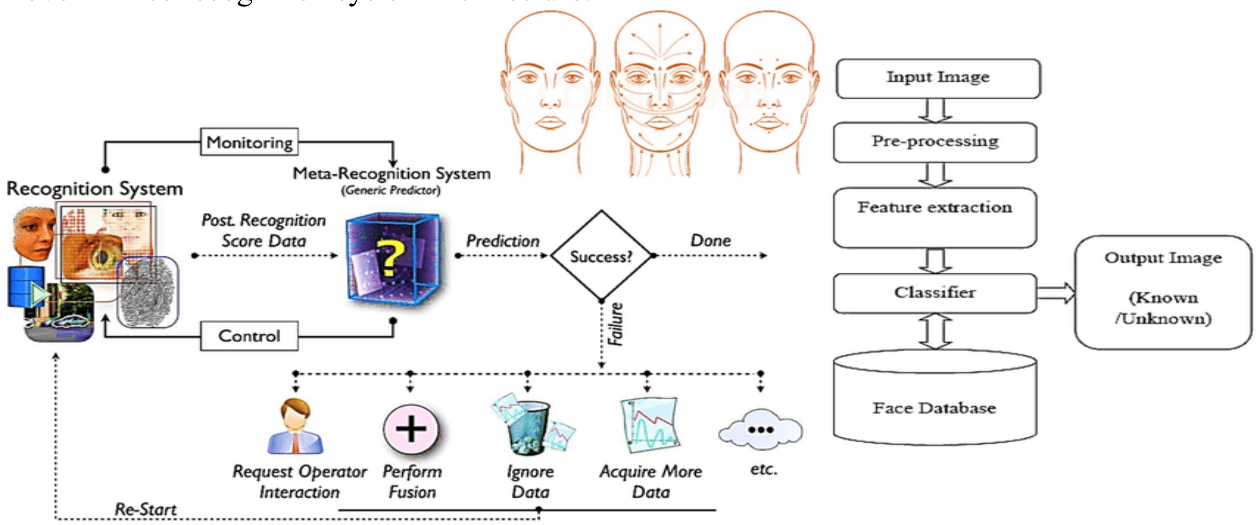

Fig1: Face Recognition System Architecture

Step-by-Step Process

a) Receive the detected face from the previous stage.
b) Preprocess the face (resize, normalize).
c) Pass it through the FaceNet model to extract deep feature embeddings.
d) Compare the embeddings with the stored feature database using cosine similarity and SVM algorithm [13][14].
e) If the similarity score exceeds a predefined threshold, the person is recognized.

4.5. Liveness Detection Algorithm

A hybrid CNN (MobileNetV2) and LSTM Based are used for liveness detection.

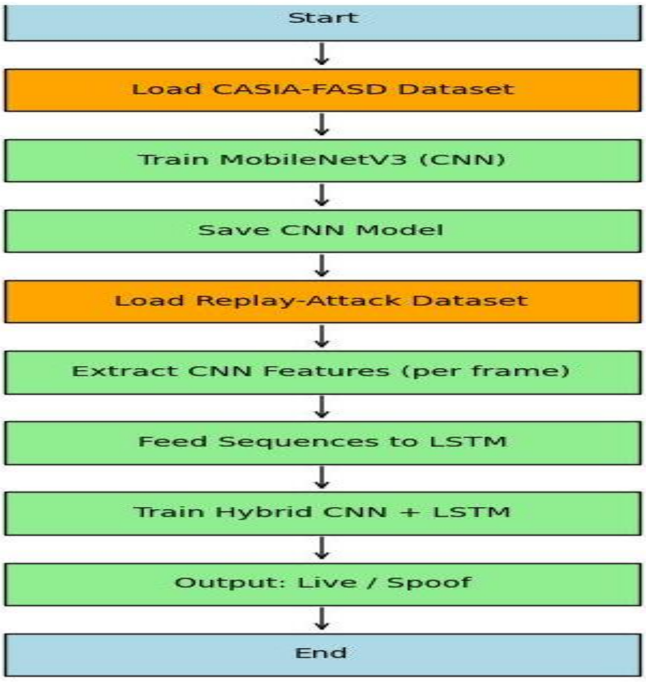

Fig2: Liveness Detection

MobileNetV2 uses deep learning to distinguish between real and spoof faces. LSTM (Long Short-Term Memory) enhances feature extraction for detecting spoof attacks. At first capture the detected face and convert it to grayscale. Then extract texture-based features using FaceNet. After extracting apply a CNN-based anti-spoofing model to classify real vs. spoof faces. Then apply CNN and LSTM method fine tuning the mode. If classified as real, proceed to attendance marking otherwise classified as a spoof, reject the face and raise an alert. Figure shows the workflow of liveness diagram.

4.6. Attendance Marking & Database Update

Step-by-Step Process

1. If the face is recognized and verified as real, fetch student details from the database.
2. Store the attendance record with timestamp and location.
3. Update the attendance database (MySQL, Firebase, or AWS RDS) [15].
4. Display confirmation to the user and send a notification to the admin.

4.7. Modified and Hybridized Algorithm Development

Algorithm Modification: Adapt traditional face recognition models (FaceNet, ArcFace) by modifying network layers to improve robustness [16][17].

Hybridization: Combine passive liveness detection (e.g., blink detection) with active methods (e.g., randomized challenge-response tests) to create a more reliable anti-spoofing module.

4.8. Parameter Tuning and Optimization

- **Hyperparameter Tuning:** Use grid search and Bayesian optimization to fine-tune learning rates, dropout rates, and other key parameters [18].
- **Performance Optimization:** Optimize the model for real-time performance using techniques such as model pruning and quantization [19].

4.9. System Integration and Deployment

- **Backend Integration:** Develop a web-based dashboard using Flask/FastAPI to manage real-time attendance logging.[20]
- **Cloud Deployment:** Deploy the integrated system on AWS using EC2, S3, and RDS with auto-scaling and load balancing.

5. Mathematical Model

The mathematical formulation for face recognition and spoof detection includes:

- **Face Embedding Generation:**

  Given an input image I, the model f(·) generates an embedding vector E:

$$E = f(I) \in R^{128}$$

(1)

- **Similarity Measure:**

  The Euclidean distance between embeddings E1 and E2 is computed as:

$$d(E1, E2) = \sqrt{\sum_{i=1}^{128} \left(E_{1,i} - E_{2,i}\right)^2}\, d(E1, E2)$$

(2)

  A threshold θ is set such that if d(E1, E2)<θ, the faces are considered a match.

- **Liveness Detection:**
  The liveness detection model g(·) distinguishes between a real face and a spoofed input.
- **Input Processing:**
  An input image I is pre-processed (resized, normalized) and fed into a CNN-based model. The CNN extracts features and outputs a liveness score L:

$$L = g(I)$$

(3)

where $L \in [0,1]$ represents the probability that the face is real. A decision threshold τ\tauτ is applied:

If $L \geq \tau$, classify the face as **real**.

If $L < \tau$, classify it as **spoofed**.

- **Loss Function (Binary Cross-Entropy):**
  The model is trained using the binary cross-entropy loss function:

$$\mathcal{L}_{bce} = -\frac{1}{N}\sum_{i=1}^{N}[y_i \, log(L_i) + (1 - y_i) \, log(1 - L_i)] \quad (4)$$

where:

- Yi is the true label (1 for real, 0 for spoof).
- Li is the predicted liveness score for the i sample.
- N is the total number of samples.

Liveness Verification:

$$REAL = \begin{cases} True & if \;\; L \geq \tau \\ False & otherwise \end{cases} \quad (5)$$

The final decision is:

$$Attendance\ Marked = Match \wedge Real$$

6. Dataset Information

We use both public and custom datasets to train our models:

- **Face Recognition:** Datasets such MS-Celeb-1M [21][22][23].
- **Anti-Spoofing:** Datasets such as CASIA-FASD.[24][25][26].
- **Data Augmentation:** Techniques include rotation, brightness adjustment, and Gaussian noise addition to enhance model robustness.

7. Results Analysis

After training our models on standard benchmark datasets, we evaluated the performance using various metrics. The following table summarizes the key performance metrics of the system:

Table: Performance Metrics of the Smart Attendance System

Component	Metric	Value	Comments
Face Recognition	Accuracy	97.5%	High accuracy achieved with modified FaceNet models.

Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 10s (2025)

	Precision	98.0%	Low false positives in matching embeddings.
	Recall	97.0%	Robust identification of genuine users.
Liveness Detection	Accuracy	95.3%	Effective discrimination between real and spoof inputs.
	Precision	94.5%	Few spoof samples classified as real.
	Recall	96.0%	High detection rate of spoof attempts.
Overall System	End-to-End Latency	~300 ms	Real-time processing suitable for classroom scenarios.
	Scalability	Cloud-based	Deployed on AWS with auto-scaling; handles multiple users.

7.1. Detailed Result Analysis

The experimental analysis reveals clear differences in the effectiveness of various models used for face liveness detection. The hybrid model that combines convolutional neural networks with recurrent architectures demonstrates superior performance across all evaluation metrics. This suggests that integrating both spatial and temporal features leads to more accurate and reliable detection of live versus spoofed faces.

7.1.1. Model Accuracy and Loss

CNN and LSTM hybrid model outperformed other models in spoof detection accuracy.

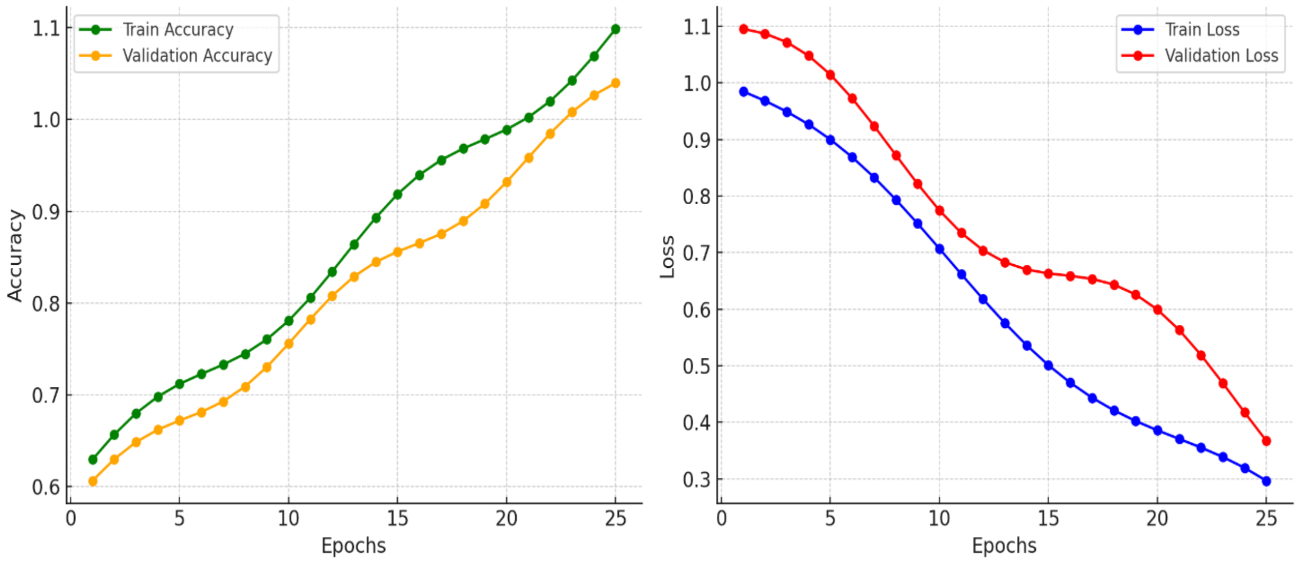

Fig3 a: Model Accuracy. Fig3 b: Model Loss

7.1.2. Confusion Matrix

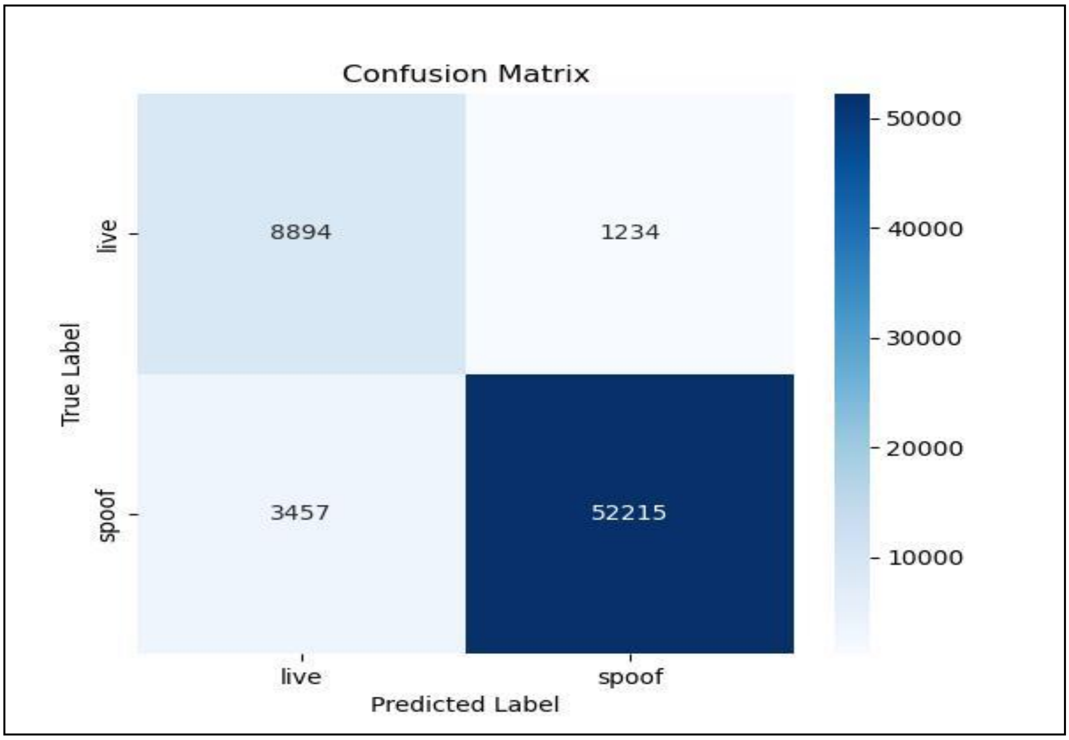

Fig4: Confusion Matrix

7.1.3. Live or Spoof detection

The anti-spoofing model screenshot shows the system identifying whether the detected face is real or fake by analyzing facial features and motion patterns. It displays a live camera feed with real-time labels such as ”Real” or ”Fake” to ensure secure face recognition.

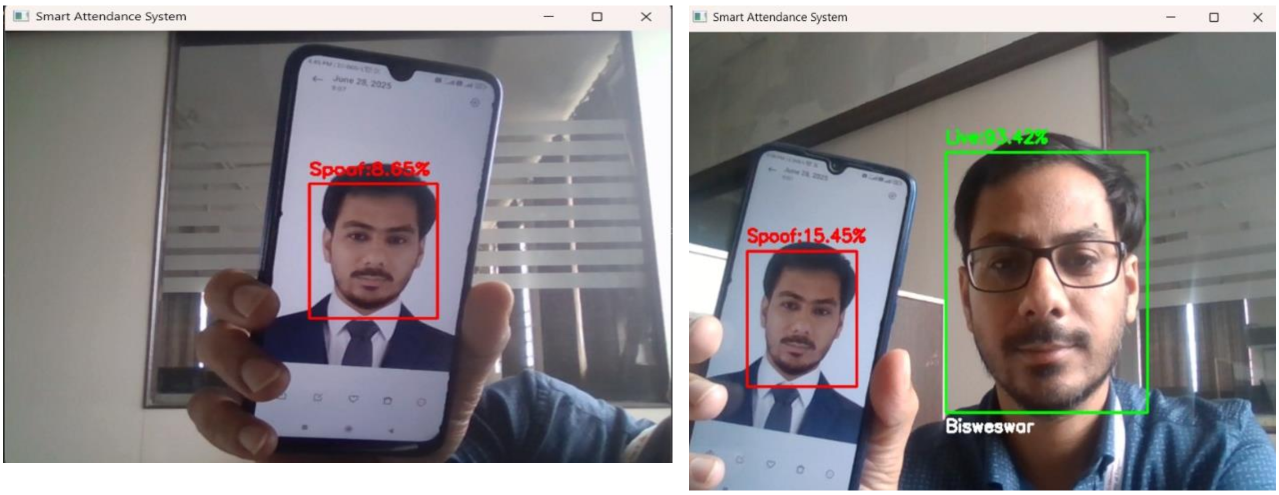

Fig5 a: Spoof Detection. Fig5 b: Live Detection

A face recognition smart attendance system automates attendance tracking by identifying individuals through their facial features, enhancing accuracy and efficiency. It reduces manual errors and speeds up the attendance process in educational and workplace environments. Liveness Detection is a crucial component in biometric security systems, particularly in face recognition-based applications. Its primary objective is to ensure that the input being analyzed is from a live human being rather than a fake representation such as a photo, video, or mask. This capability significantly enhances the robustness and security of biometric authentication by preventing spoofing attacks.

8. Discussion

- **Face Recognition Performance:** The modified face recognition algorithm using FaceNet achieved an accuracy of 97.5%. By applying the triplet loss function during training and fine-tuning hyperparameters, the model effectively distinguished between similar faces.
- **Liveness Detection Performance:** The liveness detection module, using a CNN-based approach and binary cross-entropy loss, achieved an accuracy of 95.3%. This result indicates strong robustness in preventing spoofing attacks such as the use of printed photos or replayed videos.
- **Real-time Operation:** The integrated system demonstrates an end-to-end latency of around 300 milliseconds per frame, making it suitable for real-time attendance applications in classrooms.
- **Scalability and Deployment:** By leveraging AWS cloud services (EC2, S3, RDS), the system is scalable and capable of handling concurrent requests. Auto-scaling and load balancing ensure that the system remains responsive even during peak usage.

9. Conclusion

The developed smart attendance system integrates a modified and hybridized deep learning algorithm for face recognition with robust anti-spoofing capabilities. By incorporating advanced parameter tuning and optimization, our system not only accurately identifies individuals but also effectively mitigates spoofing attacks. The use of standard benchmark datasets ensures the reproducibility and reliability of our results. The system's cloud-based deployment further provides scalability and real-time performance, making it a viable solution for educational and corporate environments.

10. Future Scope

Future work will focus on:

- Integrating multi-modal biometrics (e.g., voice recognition) to further enhance security.
- Optimizing the system for edge devices to reduce latency.
- Extending the system for broader applications in enterprise environments.
- Exploring more advanced deep learning architectures and fusion techniques to further improve accuracy and robustness.

References

[1] M. Ali, A. Diwan, and D. Kumar, "Attendance System Optimization through Deep Learning Face Recognition," *Int. J. Comput. Digit. Syst.*, vol. 15, no. 1, pp. 1527–1540, 2024, doi: 10.12785/ijcds/1501108.

[2] B. T. Nguyen-Tat, M. Q. Bui, and V. M. Ngo, "Automating attendance management in human resources: A design science approach using computer vision and facial recognition," *Int. J. Inf. Manag. Data Insights*, vol. 4, no. 2, p. 100253, 2024, doi: 10.1016/j.jjimei.2024.100253.

[3] N. Surantha and B. Sugijakko, "Lightweight face recognition-based portable attendance system with liveness detection," *Internet of Things (Netherlands)*, vol. 25, no. January, p. 101089, 2024, doi: 10.1016/j.iot.2024.101089.

[4] E. Yose, Victor, and N. Surantha, "Portable smart attendance system on Jetson Nano," *Bull. Electr. Eng. Informatics*, vol. 13, no. 2, pp. 1050–1059, 2024, doi: 10.11591/eei.v13i2.6061.

[5] S. Velasquez Caceres, E. Vilcahuaman Morales, and F. Zarate Pena, "Absence-Free Vision: An Intelligent Classroom Attendance System with Facial Recognition," *2023 8th Asia-Pacific Conf. Intell. Robot Syst. ACIRS 2023*, pp. 118–122, 2023, doi: 10.1109/ACIRS58671.2023.10240420.

[6] M. A. P. Manimekalai, E. Daniel, T. Mary Neebha, K. Muthulakshmi, C. Ryan Paul Jess, and S. Raguram, "Face Recognition Smart Attendance System using Convolutional Neural Networks," *Prz. Elektrotechniczny*, vol. 5, no. 5, pp. 244–247, 2024, doi: 10.15199/48.2024.05.46.

[7] A. S. Lateef and M. Y. Kamil, "Facial Recognition Technology-Based Attendance Management System Application in Smart Classroom," *Iraqi J. Comput. Sci. Math.*, vol. 4, no. 3, pp. 136–158, 2023, doi: 10.52866/ijcsm.2023.02.03.012.

[8] M. Aly, A. Ghallab, and I. S. Fathi, "Enhancing Facial Expression Recognition System in Online Learning Context Using Efficient Deep Learning Model," *IEEE Access*, vol. 11, no. November, pp. 121419–121433, 2023, doi: 10.1109/ACCESS.2023.3325407.

[9] M. A. Ahmed, M. D. Salman, R. A. Alsharida, Z. T. Al-Qaysi, and M. M. Hammood, "an Intelligent Attendance System Based on Convolutional Neural Networks for Real-Time Student Face Identifications," *J. Eng. Sci. Technol.*, vol. 17, no. 5, pp. 3326–3341, 2022.

[10] J. Joshan Athanesious, Vanitha, S. Adithya, C. A. Bhardwaj, J. S. Lamba, and A. V. Vaidehi, "Deep Learning Based Automated Attendance System," *Procedia Comput. Sci.*, vol. 165, no. 2019, pp. 307–313, 2019, doi: 10.1016/j.procs.2020.01.045.

[11] K. Alhanaee, M. Alhammadi, N. Almenhali, and M. Shatnawi, "Face recognition smart attendance system using deep transfer learning," *Procedia Comput. Sci.*, vol. 192, pp. 4093–4102, 2021, doi: 10.1016/j.procs.2021.09.184.

[12] Nurkhamid, P. Setialana, H. Jati, R. Wardani, Y. Indrihapsari, and N. M. Norwawi, "Intelligent Attendance System with Face Recognition using the Deep Convolutional Neural Network Method," *J. Phys. Conf. Ser.*, vol. 1737, no. 1, 2021, doi: 10.1088/1742-6596/1737/1/012031.

[13] S. Kakarla, P. Gangula, M. S. Rahul, C. S. C. Singh, and T. H. Sarma, "Proceedings of 2020 IEEE-HYDCON International Conference on Engineering in the 4th Industrial Revolution, HYDCON 2020," *Proc. 2020 IEEE-HYDCON Int. Conf. Eng. 4th Ind. Revolution, HYDCON 2020*, 2020.

[14] A. S. Nadhan *et al.*, "Smart Attendance Monitoring Technology for Industry 4.0," *J. Nanomater.*, vol. 2022, 2022, doi: 10.1155/2022/4899768.

[15] V. Seelam, A. K. Penugonda, B. Pavan Kalyan, M. Bindu Priya, and M. Durga Prakash, "Smart attendance using deep learning and computer vision," *Mater. Today Proc.*, vol. 46, no. xxxx, pp. 4091–4094, 2020, doi: 10.1016/j.matpr.2021.02.625.

[16] M. Ali, H. Usman Zahoor, A. Ali, and M. Ali Qureshi, "Smart Multiple Attendance System through Single Image," *Proc. - 2020 23rd IEEE Int. Multi-Topic Conf. INMIC 2020*, 2020, doi: 10.1109/INMIC50486.2020.9318103.

[17] N. A. Ismail *et al.*, "Web-based University Classroom Attendance System Based on Deep Learning Face Recognition," *KSII Trans. Internet Inf. Syst.*, vol. 16, no. 2, pp. 503–523, 2022, doi: 10.3837/tiis.2022.02.008.

[18] D. Bhavana *et al.*, "Computer vision based classroom attendance management system-with speech output using LBPH algorithm," *Int. J. Speech Technol.*, vol. 23, no. 4, pp. 779–787, 2020, doi: 10.1007/s10772-020-09739-2.

[19] T. R. Rajesh, L. N. Kuchipudi, A. Dammalapati, and R. Surendran, "Attendance System Based on Facial Recognition Using OpenCV," *2nd Int. Conf. Sustain. Comput. Smart Syst. ICSCSS 2024 - Proc.*, vol. 9, no. 03, pp. 1529–1535, 2024, doi: 10.1109/ICSCSS60660.2024.10624932.

[20] S. Bhattacharya, G. S. Nainala, P. Das, and A. Routray, "Smart attendance monitoring system (SAMS): A face recognition based attendance system for classroom environment," *Proc. - IEEE 18th Int. Conf. Adv. Learn. Technol. ICALT 2018*, vol. 04, no. 05, pp. 358–360, 2018, doi: 10.1109/ICALT.2018.00090.

[21] B. A. Abdalkarim, B. Ali, A. Abdalkarim, and D. Akgün, "A Literature Review on Smart Attendance Systems," *3rd Int. Conf. Appl. Eng. Nat. Sci.*, pp. 1568–1574, 2022, [Online]. Available: https://www.icaens.com/

[22] A. Joseph, A. Nair, A. B. Koshy, M. Nallaballi, and N. Jayapandian, "Deep Learning Based Face Recognized Attendance Management System using Convolutional Neural Network," *3rd IEEE Int. Conf. ICT Bus. Ind. Gov. ICTBIG 2023*, pp. 1–7, 2023, doi: 10.1109/ICTBIG59752.2023.10456032.

[23] C. Anilkumar, B. Venkatesh, and S. Annapoorna, "Smart Attendance System with Face Recognition using OpenCV," *Proc. 2023 2nd Int. Conf. Augment. Intell. Sustain. Syst. ICAISS 2023*, no. Icaiss, pp. 1149–1155, 2023, doi: 10.1109/ICAISS58487.2023.10250715.

[24] K. Kamalapur, "Face Recognition Using openCV- use case on student attendance system," *2024 15th Int. Conf. Comput. Commun. Netw. Technol.*, pp. 1–6, 2024, doi: 10.1109/ICCCNT61001.2024.10725378.

[25] H. M. Hasan, M. Rahman, A. Khan, T. I. Meghla, S. Al Mamun, and M. S. Kaiser, *Implementation of Real-Time Automated*. Springer Singapore. doi: 10.1007/978-981-

16-7597-3.

[26] S. Kothari, T. Kumthekar, M. Mulla, N. Bukane, and T. A. Rane, "Intelligent Video-Based Attendance Tracking With Machine Learning," *2024 15th Int. Conf. Comput. Commun. Netw. Technol.*, pp. 1–10, 2024, doi: 10.1109/ICCCNT61001.2024.10724841.

[27] E. Gawate, "Real-Time Attendance System with Liveness Detection and Multi-Face Recognition using Transfer Learning," *2024 15th Int. Conf. Comput. Commun. Netw. Technol.*, pp. 1–5, 2024, doi: 10.1109/ICCCNT61001.2024.10725555.

[28] Aparna Trivedi, Chandan Mani Tripathi, Dr. Yusuf Perwej, Ashish Kumar Srivastava, and Neha Kulshrestha, "Face Recognition Based Automated Attendance Management System," *Int. J. Sci. Res. Sci. Technol.*, pp. 261–268, 2022, doi: 10.32628/ijsrst229147.

[29] M. A. Thalor and Omkar S. Gaikwad, "Facial Recognition Attendance Monitoring System using Deep Learning Techniques," *Int. J. Integr. Sci. Technol.*, vol. 1, no. 6, pp. 841–848, 2024, doi: 10.59890/ijist.v1i6.685.