# Facial Recognition Based Student Attendance with Anti-Spoofing Mechanism

Akshay Santosh Torvi[1], Dandu Vijay Kumar[2], Rakasi Rohan Reddy[3], Mr.Mohammed Afzal[4]
[1,2,3]*Department of Artificial Intelligence and Machine Learning, Sphoorthy Engineering College, Hyderabad, India*
[4]*Asst.Professor, Department of CSE(AI&ML), Sphoorthy Engineering College, Hyderabad, India*

***Abstract*— Facial recognition technology has emerged as a sophisticated an efficient means of automating student attendance management systems. This paper presents a novel approach to student attendance tracking through Facial Recognition Based Student Attendance (FRBSA) integrated with an anti-spoofing mechanism. The system employs advanced facial recognition algorithms to accurately identify an authenticate students in real time and promoting a seamless a non-intrusive attendance taking process. To enhance security an prevent potential spoofing threats and an anti-spoofing mechanism has been incorporated and utilizing advanced techniques such as liveness detection to differentiate between genuine facial features a deceptive artifact. The proposed system not only streamlines attendance recording but also addresses concerns related to identity fraud an unauthorized access. The anti-spoofing measures ensure the reliability an integrity of the attendance data and contributing to the overall robustness of the system. This research not only demonstrates the feasibility an effectiveness of FRBSA in educational settings but also emphasizes the importance of incorporating anti spoofing mechanisms to bolster the security of facial recognition-based attendance systems in the evolving landscape of biometric technologies.**

***Keywords—liveness detection, unauthorized access, Biometric technologies***

## 1. INTRODUCTION

The introduction serves as a comprehensive overview, contextualizing the Facial Recognition Based Student Attendance with Anti-Spoofing Mechanism system. It begins by tracing the historical trajectory of attendance tracking methods, from manual processes to contemporary
technological solutions. The narrative highlights the inherent limitations of traditional systems, underscoring the critical need for a paradigm shift towards innovative approaches. In this digital era, the integration of facial recognition technology emerges as a transformative solution, promising not only increased efficiency but also heightened security in the realm of student attendance management. This introduction sets the stage for a detailed exploration of the proposed system and its multifaceted implications.

In this study, we propose a cost-effective solution for a camera-based attendance system applicable to both employees and students. The devised solution incorporates two Application Programming Interfaces (APIs) and a dedicated mobile application. Notably, Google's vision API is employed to detect faces within the camera frame. Once a face is detected, the mobile application transmits the captured frame to the server for subsequent processing.

Upon receiving the image, the server conducts a comparison with stored images in the database. When a match is identified, the server retrieves the corresponding employee or student's name. Real-time data exchange between the server and the mobile application is facilitated through Google's Firebase database. The instantaneous reflection of new data entries in the database and mobile application logs allows for the prompt determination of the present or absent attendance status of the employee.

### 1.1. DISTINCTIVENESS OF THE INNOVATIVE SYSTEM

In our innovative approach to camera-based detection systems, we address the challenge of marking student attendance in an online database using various techniques, including Closed-Circuit Television (CCTV) and facial recognition. Our proposed scheme stands out by offering a contact-less solution integrated with

behaviour detection, effectively capturing and thwarting spoofing attempts.

While existing studies focus on direct detection schemes for malicious actors and spoofing, we acknowledge the growing complexity of the detection mechanism as students become more adept at evading it. Specifically, challenges arise in correctly authenticating users under various attacks such as photo attacks, replay video attacks, and 3D mask attacks. Recognizing the limitations of current systems, our article introduces a novel scheme that employs an anti-spoofing mechanism leveraging open-source technologies and facial recognition through contact-less sensing.

To mitigate false positives, our system meticulously analyses a normalized dataset, identifying the genuine face by comparing it with pre-loaded trained datasets. By applying advanced techniques, we enhance the accuracy and reliability of student attendance marking, ensuring that real-user captured images and videos are correctly authenticated, even in the face of sophisticated spoofing attempts. In presenting this work, we, the authors, aim to contribute a robust solution to the evolving challenges in student attendance monitoring through state-of-the-art technology and anti-spoofing measures.

### 1.2 STUDY HIGHLIGHTS

The significant contributions of our research can be summarized as follows:

1.Introduction of a Non-Contact Attendance System: We present a cutting-edge camera-based attendance system that operates without physical contact. This system distinguishes anomalous facial images and accurately records attendance based on pre-stored data images.

2.Efficient Data Processing and Logging: Our server processes the collected images, conducts data classification and training, and systematically logs individual information along with timestamps in a secure database. This streamlined approach enhances the overall efficiency of attendance tracking.

3.Implementation of Anti-Spoofing Mechanism: To counteract the risk of spoofed images being marked in the attendance system, we incorporate a robust anti-spoofing mechanism. This mechanism, leveraging the open-source Keras Library, ensures the authenticity of identified images and guards against potential fraudulent attempts.

4. User-Friendly Mobile Application: We develop a graphical interface mobile application on the Android platform. This application facilitates user login and registration, captures facial images with appropriate pre-processing, and displays attendance marks along with other relevant information, all timestamped for reference.

## 2. THE PROPOSED SYSTEM

The architecture of the proposed system consists of five important modules that provide end-to-end monitoring of attendance based on contact-less facial detection. Fig. 1 shows the workflow process of the developed system.

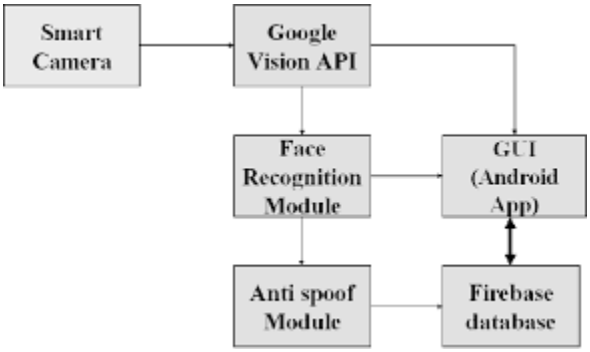


Fig. 1: Work flow of the proposed system

### 2.1 COMPUTER APPLICATION

A computer application for face scanning utilizes facial recognition technology to analyze and authenticate individuals based on facial features captured through images or live video feeds.

These applications are commonly employed for security and access control purposes, as well as in attendance tracking systems. Advanced algorithms identify unique facial patterns, enabling accurate and efficient identification within seconds.

Integration with machine learning enhances the system's ability to adapt and improve over time, providing a reliable and secure solution for identity verification.

### 2.2 DATABASE

We had integrated a database access tool within our system, utilizing the Google Firebase module. This tool ensures secure and direct access to the client-side, enabling the synchronized and responsive management of user data. Upon receiving information from the server for login or new registrations, instantaneous updates are implemented in both the Firebase database and the corresponding mobile user application.

2.3 ANTI-SPOOFING TECHNIQUES

Anti-spoofing techniques serve as a critical defense mechanism in biometric systems, particularly in the context of facial recognition technology. Spoofing refers to attempts to deceive the system by presenting fake biometric data, such as photos or videos, instead of genuine live signals. The integration of robust anti-spoofing measures is paramount to ensure the reliability and security of biometric systems.

One prevalent anti-spoofing technique is liveness detection, which aims to distinguish between genuine live subjects and deceptive artifacts. This involves analyzing dynamic cues inherent in live interactions, such as eye movement, facial expressions, or subtle physiological changes. Advanced algorithms, often based on machine learning and deep learning approaches, enable the system to discern these dynamic features and identify signs of vitality, thwarting attempts to present static images or pre-recorded videos.

Texture analysis is another prominent anti-spoofing technique that scrutinizes the unique texture patterns present on the skin. By analyzing the intricate details and irregularities in facial textures, the system can differentiate between genuine human skin and artificial materials used in spoofing attempts, such as printed photographs or silicone masks.

Additionally, the utilization of 3D facial recognition adds an extra layer of security. By capturing depth information along with surface details, the system gains a more comprehensive understanding of the facial structure, making it challenging for attackers to replicate the intricate three-dimensional aspects of a live face.

As biometric technology continues to advance, anti-spoofing techniques evolve in tandem to address emerging threats. Striking a balance between usability and security, these techniques are essential for safeguarding against potential spoofing attacks and upholding the integrity of biometric authentication systems in various domains, including access control, financial transactions, and identity verification.

Fig.2 presents the details of the SCNN network. The liveness detection takes the input as video frames and image frames and sends the input frames to the SCNN network for the liveness detection of the given input video or image frame. Fig.1 is also called as an Alpha Network, as in the non-linear diffusion code which has been implemented in the TensorFlow module is used to convert the original image to diffused form using the alpha parameter determined from the below alpha network

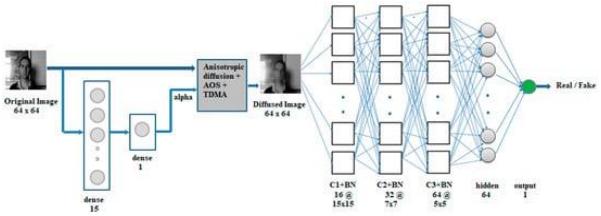


Fig.2. The architecture for Liveness Detection using SCNN

3. ALGORITHMS

Algorithm 1 Algorithm for Liveness Detection –

Input: Image Frames $I_f$ ={I1,I2,…Ik} captures from sensor.

Output: A Boolean flag to detect the detection is real or fake.

procedure LivenessDetectionSystem(video_frames):

1: Initialize liveness model
2: for each frame F_i in video_frames do
3: if F_i == φ then
4: No frames received
5: Repeat step 2
6: else
7: feature_vector_i ← ExtractFeatures(F_i)
8:liveness_score_i←liveness_model.predict(feature_vector)
9: if liveness_score_i > threshold then
10: Mark F_i as Live
11: else
12: Mark F_i as Spoofed
13: endif
14: endif
15: endfor
16: endprocedure

Explanation:

1. Initialization: Initialize the liveness detection model.
2. Iterate Over Frames: Iterate over each frame in the provided video_frames.
3. Check for Empty Frames: If a frame is empty (φ), handle the case appropriately (e.g., repeat the previous step).
4. Feature Extraction: Extract relevant features from the current frame (e.g., using CNNs).
5. Liveness Prediction: Predict the liveness of the frame using the liveness detection model. This

prediction could be a score indicating the likelihood of liveness.

6. Thresholding: Compare the liveness score with a predefined threshold. If the score exceeds the threshold, consider the frame as live; otherwise, consider it as spoofed.
7. Marking Frames: Mark the frame accordingly based on the liveness prediction.
8. Repeat or End: Repeat the process for each frame until all frames are processed.

Algorithm 2 Algorithm for Texture Analysis-
Input: Sequence of Image frames captured from the sensor SD
Output: feature vectors: Set of feature vectors containing the computed texture features of all images procedure Texture Analysis (ImageFrames):
1: Initialize denoised_images
2: for each image frame I_i in ImageFrames do
3: Denoise I_i to obtain denoised_image_i
4: Calculate gradient magnitude and orientation using Sobel operator on denoised_image_i
5: for each pixel P_ij in denoised_image_i do
6: Compute local texture features around P_ij (e.g., local binary patterns, histograms of gradients)
7: Store the computed texture features in a feature vector
8: endfor
9: endfor
10: return feature_vectors
11: endprocedure

Explanation:

- ImageFrames (If): Represents the sequence of image frames captured from the sensor (SD).
- I_i: Represents an individual image frame in the sequence.
- denoised_images: Denotes the set of images obtained after applying denoising techniques to each image frame.
- gradient magnitude: Represents the magnitude of gradient computed using the Sobel operator.
- gradient orientation: Denotes the orientation of gradient computed using the Sobel operator.
- P_ij: Represents an individual pixel in the denoised image.
- local texture features: Refers to the features computed based on the local characteristics of the image, such as local binary patterns (LBP) or histograms of gradients (HOG).
- feature_vectors: Represents the set of feature vectors containing the computed texture features for all image frames.

Algorithm 1, focused on liveness detection, begins by capturing a sequence of video frames. Each frame undergoes analysis to extract features indicative of liveness, such as facial movements or physiological signals. Subsequently, a machine learning model, trained to differentiate between live faces and spoofing attempts, is employed. Finally, the model's output is evaluated to determine whether the presented face is live or spoofed.

In contrast, Algorithm 2 centers on texture analysis. It involves processing the image to extract local texture features, encompassing gradients, edges, or patterns. Techniques like GLCM or LBP are then applied to quantify the distribution and relationships of these features. Subsequently, statistics or histograms are computed from the extracted features, serving to represent the texture properties of the image. These descriptors find utility in various tasks, including image classification, segmentation, or object recognition.

Fig.3. Shows the actual person trying to login and the system recognizes him as real. Fig.4.shows the fake identity photo trying to login into the system.

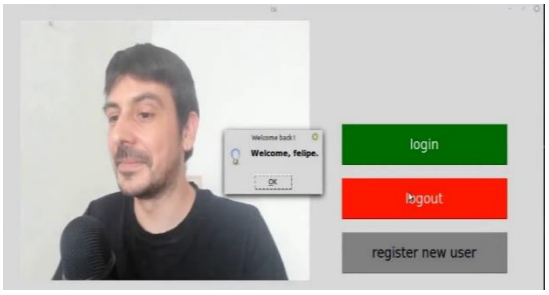


Fig.3. Actual Person Trying to login

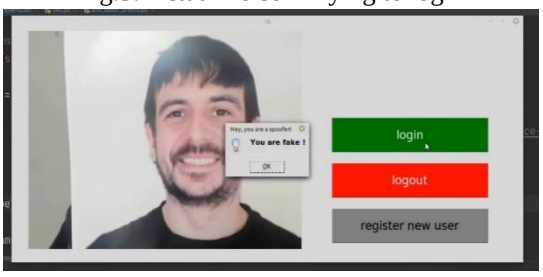


Fig.4. Person trying to spoof using his image

First the user gets to register his Face image to the application, and the application will store his image in the database and further will rectify the image with the images in the database and marks the attendance for the student for the day. If someone tries to attack with a photograph or an video of the existing user in the database, the application will use the following Anti-Spoofing Techniques in identifying the fake image and demarks the attendance and the organization or the administration will get to know that a student is trying to spoof.

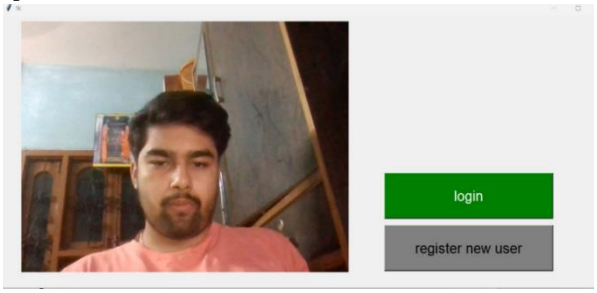


Fig.5. Application's UI login Page


Fig.6. Registration Page

Registration Steps:

1. User Initiation: The user initiates the registration process by accessing the registration page or section of the facial recognition system.
2. Facial Data Collection: The system prompts the user to provide facial data by capturing multiple images of their face from different angles.
3. Facial Feature Extraction: Advanced algorithms within the system analyze the captured images to extract unique facial features, such as key points, distances between facial landmarks, and other relevant data.
4. Creation of Facial Template: Using the extracted facial features, the system generates a unique facial template or signature that represents the user's face. This template is securely stored in the system's database.
5. Database Entry: The system stores the generated facial template along with other user information in the database, associating it with the user's account.
6. Confirmation: Optionally, the system may provide a confirmation message to the user, indicating the successful registration process.

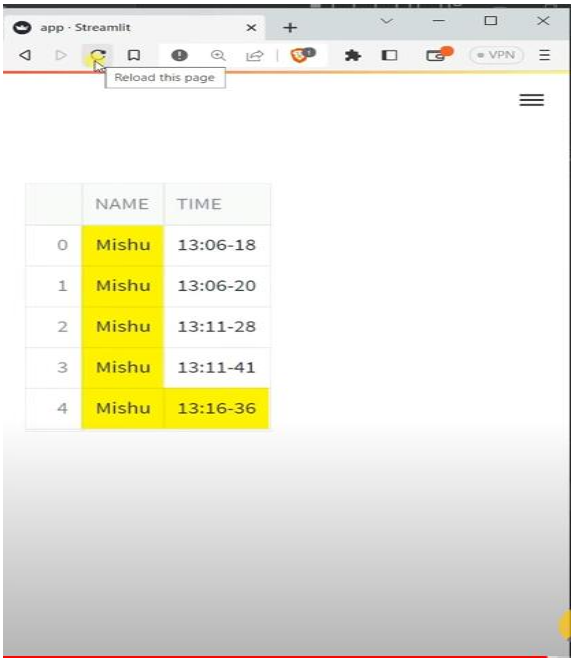


Fig.7. User Log

## 4. EVALUATION

### 4.1 DATASETS

A dataset is a structured collection of data generally associated with a unique body of work. A database is an organized collection of data stored as multiple datasets. It is a collection of numbers, text that relate to a particular subject. Following are the datasets of our Facial Recognition to recognize the faces which are been registered by the candidates or have been taken from the organization.


Fig.8. Database of Registered Faces

4.2 EVALUATION MATRIX

Evaluating models is a crucial step in machine learning and data science. It helps assess how well a model is likely to perform on unseen data. Choose appropriate evaluation metrics based on the problem type and dataset. It used to assess the real-world impact of the model's predictions on the business objective. An evaluation metric quantifies the performance of a predictive model. This typically involves training a model on a dataset, using the model to make predictions on a holdout dataset not used during training, then comparing the predictions to the expected values in the holdout dataset.

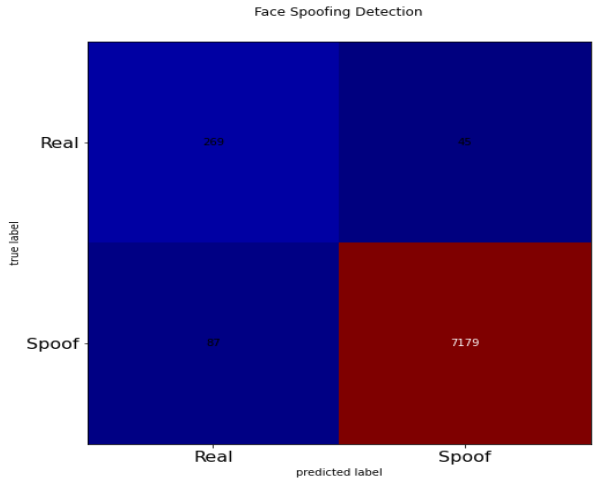


Fig.9. Analysis Between Fake and Real detected

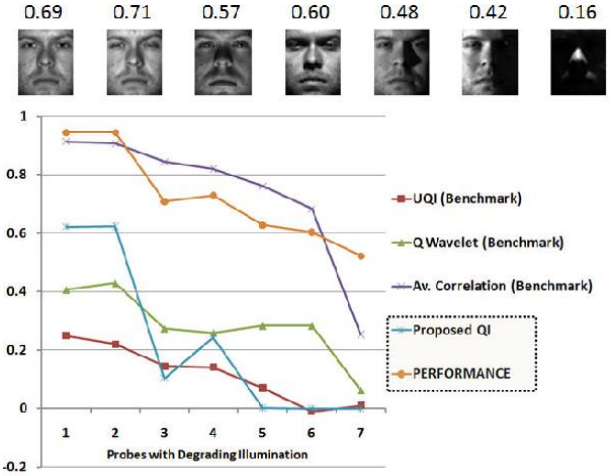


Fig.10. Performance Analysis

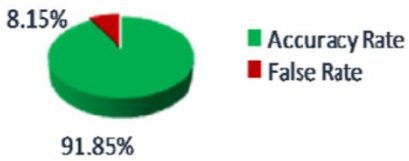


Fig. 11. Accuracy

4.3 ANALYSIS OF ANTI-SPOOFING TECHNIQUES

- In this segment, the effectiveness of the proposed CNN-LSTM approach is evaluated against existing methodologies. Specifically, we compare our scheme with Sajida et al. [12], which introduces the Dynamic Local Ternary Pattern (DLTP), and Tan et al. [21], which presents the Difference-of-Gaussian (DoG) technique. Our analysis encompasses the variation of learning rate (η) and diffusion parameter (α) within the CNN-LSTM network architecture. Detailed findings are elucidated as follows.

**Table-1** Accuracy of proposed system for diffused images

| Diffused Images (Param $\alpha$) | Epochs | CNN-5 | Epochs | ResNet50 |
|---|---|---|---|---|
| 15 | 25 | 88.69 | 40 | 78.76 |
| 25 | 30 | 95.99 | 20 | 95.86 |
| 50 | 20 | 79.44 | 30 | 70.21 |
| 75 | 20 | 76.35 | 30 | 78.77 |
| 100 | 30 | 75.77 | 30 | 74.47 |

- The accuracy metrics of the proposed scheme for diffused images (α values) across CNN-5 and ResNet-50 models are presented in Table 3. The performance of the models across different epochs is evaluated to gauge their effectiveness in handling diffused images. Notably, ResNet-50 exhibits superior computational speed owing to skip connections, facilitating faster gradient propagation through dense layers. Conversely, CNN-5 achieves higher accuracy in specific α values, benefiting from reduced parameter exchange in intermediate layers.
- Additionally, a comparative analysis against state-of-the-art schemes, namely DLTP [12] and DoG [21], is conducted on the NUAAdataset. Table 4 showcases the outcomes of this comparison, revealing the superior performance of our proposed ResNet-50 model in liveness detection, achieving an accuracy of 95.85%. This achievement surpasses the accuracies attained by DLTP (94.5%) and DoG (87.5%). The resilience of the CNN-LSTM architecture to image variations, coupled with its spatial information processing capability, contributes to the extraction of discriminative features essential for effective liveness detection.
- The accuracy of the detection of spoofed images are identified and gives the accuracy of our system and ability to detect the attack and ensure a smooth run of the smart attendance system.

## 5. CONCLUSION

The paper introduces an innovative contactless attendance scheme tailored to modern requirements, prioritizing social distancing norms. It effectively addresses the challenge of detecting suspicious spoofing attempts involving reproduced or still images, thus mitigating the risk of photo replay attacks. Leveraging open-source APIs, the scheme employs the dlib library for robust face recognition and the Google Vision API for rapid image matching against stored datasets.

A key feature of the system is its liveness detection module, powered by an LSTM-CNN network designed to discern between genuine and fabricated facial representations. Through meticulous analysis of discriminative facial features, this module accurately classifies presented images as either authentic or fake. Furthermore, the paper presents a demonstration of a mobile application equipped with registration and scanning modules, facilitating seamless user check-in and check-out procedures while maintaining comprehensive logs.

Looking ahead, the authors outline a promising future scope for the system. They propose the incorporation of transfer learning techniques to further refine the system's performance by leveraging the wealth of knowledge accumulated from facial images. Specifically, the integration of an InceptionV4 network is envisioned to enhance the accuracy and reliability of the marking system, underscoring the commitment to continuous improvement and innovation in attendance management.