Deep Learning-Based Face Authentication for Secure Attendance Applications

J.Karthik [1],M.Anusha[2]
[1]MCA Student , Dept of MCA , Ellenki College of Engineering and Technology , Hyderabad
[2]Assistant Professor , Dept of MCA , Ellenki College of Engineering and Technology , Hyderabad

***Abstract*—** Face-based attendance systems are widely adopted because they automate identity verification and reduce manual record keeping. However, conventional facial recognition systems remain susceptible to presentation attacks such as printed photographs, replay videos, and mobile screen images, which can result in unauthorized attendance marking. This paper presents a CNN-based anti-spoofing face attendance framework that combines robust facial authentication with real-time attendance management. The proposed approach performs image preprocessing using YCrCb and CIE L*uv** colour spaces to extract discriminative histogram features that effectively separate genuine facial characteristics from spoof artefacts. These features are supplied to a Convolutional Neural Network (CNN) for live face verification before the recognition stage. Once a face is confirmed as genuine, facial embeddings are generated and matched with registered user encodings to identify individuals accurately. A web-based application has been developed with modules for administrator authentication, user registration, secure attendance marking, attendance monitoring, and user management. Attendance records are automatically stored in a MySQL database with corresponding date and time information for future reference. Experimental evaluation demonstrates that the proposed framework successfully distinguishes real faces from spoof attempts while maintaining reliable recognition performance under practical operating conditions. The integration of anti-spoofing verification with automated attendance management provides a secure, efficient, and scalable solution suitable for educational institutions, workplaces, and other access-controlled environments.

***Keywords*—** Convolutional Neural Network (CNN), face anti-spoofing, facial recognition, biometric authentication, attendance management system, YCrCb colour space, CIE L*uv** colour space, histogram feature extraction, face detection, liveness detection, OpenCV, real-time attendance monitoring, facial embeddings, MySQL database, secure access control.

I.INTRODUCTION

Automated attendance systems have become an integral part of educational institutions, corporate organizations, and secure workplaces due to their ability to reduce manual effort and improve record

management. Among the available biometric technologies, facial recognition has gained widespread acceptance because it enables contactless identification and provides a convenient user experience. Despite these advantages, conventional face recognition systems remain vulnerable to presentation attacks, where printed photographs, replay videos, or images displayed on mobile devices are used to impersonate authorized individuals **[3]**. Such spoofing attacks can compromise attendance records and reduce the reliability of biometric authentication systems. Consequently, there is a growing need for attendance solutions that can accurately distinguish genuine users from fraudulent attempts while maintaining high recognition accuracy and operational efficiency **[10]**.

Recent advances in deep learning have significantly improved the capability of biometric security systems to detect spoofing attacks. Convolutional Neural Networks (CNNs) have demonstrated strong performance in extracting discriminative image features required for liveness detection **[4], [5]**. In addition, colour-space analysis has proven effective for identifying subtle differences between real human skin and presentation attacks. By transforming facial images into YCrCb and CIE L*uv** colour spaces, luminance and chrominance information can be analysed independently, allowing histogram-based feature extraction to capture characteristics that are difficult to observe in the conventional RGB colour model. The extracted features are subsequently utilized by the CNN model to classify facial samples as either genuine or spoof before the identity verification process is performed. This layered verification strategy enhances the security and robustness of facial authentication systems **[9]**.

This work presents a CNN-based anti-spoofing face attendance system tht integrates liveness detection, facial recognition, and automated attendance management within a secure web application. The proposed framework incorporates administrator authentication, user registration, face encoding generation, real-time attendance marking, attendance monitoring, and user management functionalities **[13]**. During attendance verification, the system first validates the authenticity of the

detected face using CNN-based anti-spoofing and then performs facial recognition by matching facial embeddings with registered user encodings. Successfully verified attendance records are automatically stored in a MySQL database along with the corresponding date and time information for future reference. The proposed solution provides an effective, scalable, and secure attendance management framework capable of preventing common spoofing attacks while ensuring reliable identity verification in real-world environments **[6]**.

II.RELATED WORK

K. Ito, T. Okano, and T. Aoki (2017) presented "Recent Advances in Biometric Security: A Case Study of Liveness Detection in Face Recognition" [1]. The study examined the importance of liveness detection in improving the security of face recognition systems against presentation attacks. Various biometric verification techniques were discussed to distinguish genuine users from spoofing attempts involving photographs and digital displays. The authors emphasized that integrating liveness verification with facial authentication significantly improves system reliability and reduces unauthorized access. Their work highlighted the growing role of biometric security in real-world authentication applications. [1]

P. Anthony, B. Ay, and G. Aydin (2021) proposed "A Review of Face Anti-Spoofing Methods for Face Recognition Systems" [2]. The authors surveyed different anti-spoofing approaches developed to protect face recognition systems from presentation attacks. The review compared traditional image processing methods with deep learning-based techniques and discussed their effectiveness under different attack scenarios. The study concluded that convolutional neural network models provide superior performance by learning discriminative facial characteristics from large datasets. The review also identified future challenges in developing robust and generalized anti-spoofing solutions. [2]

A. A. Mohamed, M. M. Nagah, M. G. Abdelmonem, M. Y. Ahmed, M. El-Sahhar, and F. H. Ismail (2021) proposed "Face Liveness Detection Using a Sequential CNN Technique" [4]. The proposed method employed a sequential convolutional neural network to classify facial images as either genuine or spoofed. The model automatically extracted representative image features without requiring handcrafted descriptors, enabling efficient liveness verification. Experimental evaluation demonstrated that the CNN-based approach achieved reliable classification performance under different presentation attack conditions. The study showed that deep learning techniques can substantially strengthen the security of face recognition systems. [4]

R. B. Hadiprakoso, H. Setiawan, and Girinoto (2020) presented "Face Anti-Spoofing Using CNN Classifier and Face Liveness Detection" [5]. The research introduced a CNN-based classification framework for identifying spoofing attacks before facial recognition was performed. The proposed system analyzed facial characteristics to differentiate genuine users from printed photographs and replay attacks. By combining liveness detection with facial authentication, the framework improved recognition reliability and minimized the possibility of unauthorized access. The experimental results confirmed the effectiveness of CNN models in enhancing biometric security. [5]

M. Arsenovic, S. Sladojevic, A. Anderla, and D. Stefanovic (2017) proposed "FaceTime—Deep Learning Based Face Recognition Attendance System" [10]. The authors developed an automated attendance management system that utilized deep learning techniques for facial recognition. The system captured facial images, identified registered individuals, and automatically recorded attendance without requiring manual intervention. The proposed approach reduced errors associated with conventional attendance methods while providing a faster and more convenient authentication process. The study demonstrated that deep learning-based face recognition offers an efficient solution for real-time attendance management. [10]

III.DATASET DETAILS

The proposed CNN-based anti-spoofing face attendance system utilizes a facial image dataset consisting of genuine face samples and spoof face samples collected under different presentation conditions. The dataset contains images captured from real users through a webcam as well as spoofing attempts created using printed photographs and mobile screen displays. Each registered user is assigned a unique person ID, and multiple facial images are captured during the registration process to generate facial encodings for identity verification. These images form the reference database used for subsequent recognition and attendance marking. Before model training, the collected images undergo preprocessing to improve their suitability for anti-spoofing analysis. The preprocessing stage converts facial images from the conventional RGB colour space into YCrCb and CIE L*u*v* colour spaces, allowing luminance and chrominance information to be analyzed separately. Histogram features extracted from these colour spaces provide discriminative information that assists the CNN model in distinguishing genuine faces from presentation attacks. This preprocessing process enhances feature consistency while improving the robustness of the liveness detection framework. The processed facial image dataset is used to train a Convolutional Neural

Network (CNN) for anti-spoofing classification. During training, the CNN learns representative feature patterns associated with real and spoof facial images without relying on manually designed descriptors. Once training is completed, the model evaluates incoming facial images captured by the webcam and classifies them as either genuine or spoof. Only images identified as genuine are forwarded to the face recognition module, where facial embeddings are generated and compared with the stored encodings of registered users. This two-stage verification process significantly reduces the possibility of unauthorized attendance caused by printed photographs, replay attacks, or mobile screen images while maintaining reliable recognition performance. The same dataset also supports the real-time operation of the developed attendance management application. During user registration, facial images and corresponding encoding files are securely stored for future authentication. When attendance is initiated, the webcam captures live facial images, performs anti-spoofing verification, and recognizes authenticated users before automatically recording attendance information in the MySQL database along with the corresponding date and time. The database also maintains user registration details, attendance history, and management records, enabling administrators to search attendance information, monitor user activity, and manage registered users efficiently. The integration of a structured facial image dataset, CNN-based liveness detection, facial recognition, and automated attendance management provides a secure and scalable solution for preventing spoofing attacks while ensuring accurate real-time attendance recording.

IV.PROPOSED METHODOLOGY

The proposed framework presents a secure face attendance system that integrates Convolutional Neural Network (CNN)-based anti-spoofing with facial recognition to ensure reliable and unauthorized attendance prevention. The objective of the system is to verify both the authenticity and identity of an individual before recording attendance. A web-based application is developed to provide administrator authentication, user registration, attendance marking, attendance monitoring, and user management within a unified platform. The framework combines image preprocessing, liveness detection, face recognition, and database management to deliver an efficient and secure attendance solution.

The methodology begins with user registration, where the administrator enters a unique person ID and user name while the system captures multiple facial images through a webcam. The captured images are preprocessed by converting them into YCrCb and CIE L*uv** colour spaces, enabling effective separation of luminance and chrominance information. Histogram features extracted from these colour spaces are supplied to the CNN model, which learns discriminative characteristics of genuine and spoof facial images. Once the CNN confirms that the detected face is genuine, facial embeddings are generated and compared with the stored encoding files of registered users to establish identity accurately.

During attendance marking, the webcam continuously captures live video frames and performs face detection using OpenCV and facial recognition techniques. Each detected face is first evaluated by the CNN-based anti-spoofing model to determine whether it represents a real person or a presentation attack such as a printed photograph or mobile display. Only genuine faces are forwarded to the recognition module for identity matching. After successful authentication, the attendance details, including user ID, date, time, and attendance status, are automatically recorded in the MySQL database. The administrator can subsequently view attendance records, search user details, or remove registered users through the management interface. The integration of CNN-based liveness detection, facial recognition, and automated database management provides a scalable, accurate, and secure attendance system capable of minimizing spoofing attacks while supporting reliable real-time attendance recording.

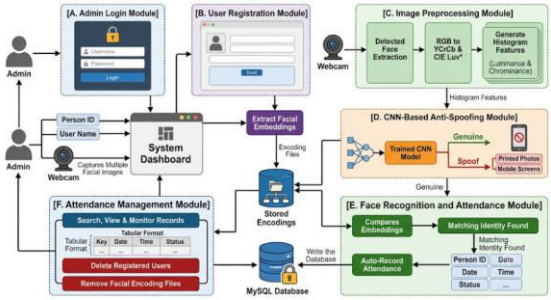

Figure 1: System Architecture of the Proposed CNN-Based Anti-Spoofing Face Attendance System

Figure 1 presents the overall architecture of the proposed CNN-based anti-spoofing face attendance system. The workflow begins with the Admin Login module, where the administrator securely accesses the application to manage users and attendance records. Through the User Registration module, the administrator enters the user's unique person ID and name, while the webcam captures multiple facial images to generate facial embeddings. These embeddings are stored as encoding files and serve as reference templates for future identification. Before recognition, every captured facial image is processed by the Image Preprocessing module, where the detected face is converted into YCrCb and CIE L*uv** colour spaces. Histogram features extracted from these colour channels are supplied to the CNN-based Anti-Spoofing module, which

determines whether the detected face is genuine or a spoofing attempt, such as a printed photograph or a mobile screen image. Only genuine faces proceed to the recognition stage. The Face Recognition and Attendance module compares the extracted facial embedding with the stored encodings to identify the registered user. After successful authentication, the system automatically records the attendance details, including person ID, date, time, and attendance status, in the MySQL database. Finally, the Attendance Management module enables the administrator to search attendance records, monitor user attendance, and remove registered users along with their associated facial encoding files. The integration of image preprocessing, CNN-based liveness detection, facial recognition, and database management provides a secure, reliable, and efficient framework for real-time attendance monitoring while minimizing spoofing attacks.

V.RESULT AND DISCUSSION

The proposed CNN-based anti-spoofing face attendance system was evaluated using the developed web application under different real-time operating conditions. The application successfully performed administrator authentication, user registration, facial image acquisition, anti-spoofing verification, face recognition, attendance recording, and attendance management through an integrated interface. During user registration, multiple facial images were captured through a webcam, and corresponding facial encoding files were generated and stored for subsequent identity verification. The registration process was completed successfully for all enrolled users, demonstrating the reliability of the facial enrollment mechanism. The administrator was also able to manage user information and monitor attendance records efficiently through the system dashboard.

The anti-spoofing module effectively distinguished genuine users from presentation attacks by analyzing histogram features extracted from the YCrCb and CIE L*u*v* colour spaces using the trained CNN model. When a live user appeared before the webcam, the system correctly identified the face as genuine and allowed the recognition process to continue. In contrast, when printed photographs or facial images displayed on mobile screens were presented to the camera, the CNN model classified them as spoof attempts and denied attendance. This verification stage significantly reduced the possibility of unauthorized attendance marking and improved the overall security of the biometric authentication process.

After successful liveness verification, the face recognition module accurately matched facial embeddings with the stored encoding files of registered users. Once a valid match was identified, the application automatically recorded attendance by storing the person's identification number, attendance date, attendance time, and attendance status in the MySQL database. The attendance records were immediately available through the administrator interface, allowing efficient searching and monitoring of user attendance history. The delete user module also functioned correctly by removing registered user information, facial encoding files, and related attendance records whenever required.

The experimental observations indicate that the integration of image preprocessing, CNN-based liveness detection, facial recognition, and automated database management provides a secure and dependable attendance solution for real-world applications. The developed framework successfully prevents common spoofing attacks while maintaining reliable recognition performance and efficient attendance recording. These results demonstrate that the proposed system is suitable for educational institutions, offices, and other organizations requiring secure, contactless, and real-time attendance management.

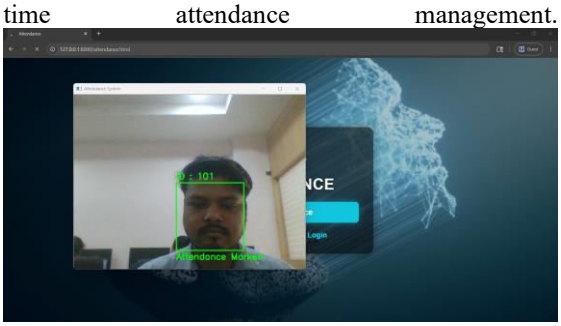

Figure 2: Successful Face Recognition and Attendance Marking

Figure 2 shows the successful execution of the proposed CNN-based anti-spoofing face attendance system during the attendance verification process. After the user initiates attendance, the webcam captures a live facial image and detects the face in real time. The captured face is first analyzed by the CNN-based anti-spoofing module to verify that it belongs to a genuine user rather than a spoofing source such as a printed photograph or mobile screen image. Once the liveness verification is completed successfully, the face recognition module compares the extracted facial features with the stored facial encodings of registered users. When a valid match is found, the user's identity is displayed on the screen, and the message **"Attendance Marked"** confirms that the attendance has been recorded successfully. The corresponding attendance information, including the user ID, date, time, and attendance status, is automatically stored in the MySQL database. This result demonstrates that the proposed framework performs accurate real-time facial authentication while preventing unauthorized attendance and ensuring secure attendance management.

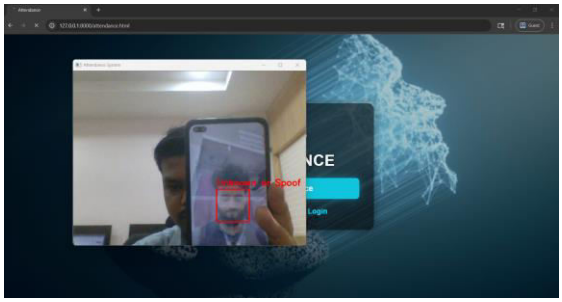

Figure 3: Detection of Spoof Attack During Attendance Verification

Figure 3 illustrates the anti-spoofing capability of the proposed CNN-based face attendance system when a spoofing attempt is made using a mobile phone displaying a facial image. During the attendance process, the webcam captures the presented face and forwards the detected facial region to the CNN-based anti-spoofing module for liveness verification. Instead of identifying the displayed image as a genuine face, the model correctly recognizes it as a presentation attack and displays the message **"Unknown or Spoof."** Since the detected input fails the liveness verification stage, the face recognition module is not executed, and attendance is not recorded. This result demonstrates that the proposed system can effectively detect spoofing attempts involving mobile screen images, thereby preventing unauthorized attendance marking. The successful rejection of fake facial inputs confirms the effectiveness of the integrated CNN-based liveness detection mechanism in improving the security and reliability of the attendance management system.

DISCUSSION

The proposed face attendance framework integrates CNN-based anti-spoofing, facial recognition, and automated attendance management to provide secure and reliable biometric authentication. The system utilizes image preprocessing through YCrCb and CIE L*uv** colour spaces to extract discriminative histogram features, which are supplied to a Convolutional Neural Network (CNN) for liveness verification. Only facial images classified as genuine are forwarded to the recognition module, where facial embeddings are compared with stored user encodings to verify identity. A web-based application incorporates administrator authentication, user registration, real-time attendance marking, attendance monitoring, and user management within a single platform.

Experimental results demonstrate that the proposed framework accurately distinguishes genuine users from spoofing attempts involving printed photographs and mobile screen images while maintaining dependable face recognition performance. The integration of CNN-based liveness detection with facial recognition effectively prevents unauthorized attendance and improves the security of the authentication process. Furthermore, attendance records are automatically stored in a MySQL database with the corresponding user ID, date, time, and attendance status, enabling efficient record management and monitoring. The proposed system therefore provides a practical, scalable, and secure solution for real-time attendance management, making it well suited for educational institutions, workplaces, and other environments that require reliable biometric attendance recording.

VI.CONCLUSION

This work presents a CNN-based anti-spoofing face attendance system that combines liveness detection, facial recognition, and automated attendance management to provide a secure and dependable biometric authentication framework. The proposed system employs image preprocessing using YCrCb and CIE L*uv** colour spaces together with a Convolutional Neural Network (CNN) to distinguish genuine facial inputs from spoofing attempts before identity verification is performed. The developed web-based application incorporates administrator authentication, user registration, real-time attendance marking, attendance monitoring, and user management within a single platform. Experimental evaluation demonstrates that the system successfully identifies legitimate users while effectively rejecting presentation attacks involving printed photographs and mobile screen images. Attendance records are automatically stored with the corresponding user details, date, time, and attendance status, ensuring accurate and efficient attendance management. The proposed framework provides a practical, scalable, and secure solution for organizations requiring reliable contactless attendance systems. Future work may focus on improving the anti-spoofing model by incorporating advanced deep learning architectures, supporting additional presentation attack types such as replay videos and 3D masks, integrating cloud-based attendance services, and extending the system to operate efficiently across diverse environmental conditions and large-scale user deployments.

REFERENCES

[1] K. Ito, T. Okano, and T. Aoki, “Recent advances in biometric security: A case study of liveness detection in face recognition,” in 2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), 2017, pp. 220–227.

[2] P. Anthony, B. Ay, and G. Aydin, “A review of face anti-spoofing methods for face recognition systems,” in 2021 International Conference on

Innovations in Intelligent Systems and Applications (INISTA), 2021, pp. 1–9.

[3] M. Bagga and B. Singh, “Spoofing detection in face recognition: A review,” in 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016, pp. 2037–2042.

[4] A. A. Mohamed, M. M. Nagah, M. G. Abdelmonem, M. Y. Ahmed, M. El-Sahhar, and F. H. Ismail, “Face liveness detection using a sequential CNN technique,” in 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 2021, pp. 1483–1488.

[5] R. B. Hadiprakoso, H. Setiawan, and Girinoto, “Face anti-spoofing using CNN classifier and face liveness detection,” in 2020 3rd International Conference on Information and Communications Technology (ICOIACT), 2020, pp. 143–147.

[6] R. Ganjoo and A. Purohit, “Anti-spoofing door lock using face recognition and blink detection,” in 2021 6th International Conference on Inventive Computation Technologies (ICICT), 2021, pp. 1090–1096.

[7] T. Soukupova and J. Cech, “Real-time eye blink detection using facial landmarks,” 2016.

[8] M. P. Beham, S. M. M. Roomi, H. Jebina, and M. Kavitha, “Face spoofing detection using binary gradient orientation pattern with deep neural network,” in 2017 Ninth International Conference on Advances in Pattern Recognition (ICAPR), 2017, pp. 1–6.

[9] L. Song and H. Ma, “Face liveliness detection based on texture and color features,” in 2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), 2019, pp. 418–422.

[10] M. Arsenovic, S. Sladojevic, A. Anderla, and D. Stefanovic, “FaceTime—Deep learning based face recognition attendance system,” in 2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY), 2017, pp. 53–58.

[11] S. Kakarla, P. Gangula, M. Rahul, C. S. C. Singh, and T. H. Sarma, “Smart attendance management system based on face recognition using CNN,” in 2020 IEEE HYDCON, 2020, pp. 1–5.

[12] E. Winarno, I. Husni Al Amin, H. Februariyanti, P. W. Adi, W. Hadikurniawati, and M. T. Anwar, “Attendance system based on face recognition using CNN-PCA method and real-time camera,” in 2019 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 2019, pp. 301–304.

[13] S. Huang and H. Luo, “Attendance system based on dynamic face recognition,” in 2020 International Conference on Communications, Information System and Computer Engineering (CISCE), 2020, pp. 368–371.

[14] J. Cech and T. Soukupova, “Real-time eye blink detection using facial landmarks,” Cent. Mach. Perception, Dep. Cybern. Fac. Electr. Eng. Czech Tech. Univ. Prague, pp. 1–8, 2016.

[15] F. Schroff, D. Kalenichenko, and J. Philbin, “FaceNet: A unified embedding for face recognition and clustering,” in 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015, pp. 815–823.