IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 11, April 2025

Impact Factor: 7.67

Face Recognition Attendance System with Anti-Spoofing Detection

Dr Shabeena Sayed[1], Shaikh Fatima[2], Qureshi Abdul kader[3],
Morkas Ebrahim[4], Shaikh Mohammed Ibrahim[5]
Guide, Dept. of Information Technology[1]
Students, Dept. of Information Technology[2,3,4,5]
M.H. Saboo Siddik College of Engineering, Mumbai

Abstract: *In this project, we are developing a Face Recognition Based Attendance System with Anti-Spoofing Detection that utilizes advanced computer vision techniques to automate the process of taking attendance in educational and corporate settings. The system captures and recognizes the faces of individuals to mark their presence, ensuring accuracy and efficiency. To enhance security and prevent fraudulent attendance, we are implementing anti spoofing detection measures. This feature distinguishes between real faces and spoofing attempts, such as photos or videos, thereby ensuring the integrity of the attendance records. The system aims to provide a reliable and user-friendly solution for attendance management, integrating face recognition technology with robust anti-spoofing capabilities. The final product promises to enhance the efficiency of attendance management, reduce administrative workload, and provide accurate records while maintaining user privacy*

Keywords: Anti-Spoofing Detection, Attendance System, Face Recognition, Corporate Attendance, Automated Attendance

I. INTRODUCTION

The traditional methods of attendance tracking, such as roll calls or paper-based registers, are often time-consuming and prone to errors. With the rapid advancement of technology, there is a growing need for automated systems that can streamline the attendance process. Face Recognition Attendance Systems have emerged as an innovative solution to this challenge, leveraging the capabilities of artificial intelligence (AI) and machine learning (ML) to accurately identify individuals in real-time. Face recognition technology involves capturing an image of a person’s face and comparing it against a database of stored images to verify their identity. This biometric method is not only efficient but also minimizes human intervention, thereby reducing the chances of errors associated with manual attendance systems. The widespread availability of cameras and the increasing affordability of computing devices have further accelerated the adoption of this technology in various sectors, including education, corporate environments, and public services. To enhance security and prevent fraudulent activities, such as using photos, videos, or masks to spoof the system, anti-spoofing techniques are integrated. Anti-spoofing detection can use methods like liveness detection, which analyses real-time cues (e.g., eye blinks, 3D face depth, or skin texture), to distinguish between a real person and a fake representation. This combination of face recognition with anti-spoofing ensures both accuracy and security in attendance tracking, reducing the risk of manipulation while improving efficiency.

II. LITERATURE REVIEW

Face recognition-based attendance systems have witnessed significant development, with researchers focusing not only on accurate recognition but also on enhancing security against spoofing attacks. This section reviews existing methods, highlighting their techniques, advantages, and limitations. In comparison, the current project employs MobileNetV3, a lightweight and efficient deep learning model, optimized for real-time anti-spoofing detection. The MobileNetV3 model delivers a balance between high accuracy and fast processing, making it suitable for web and mobile environments where

DOI: 10.48175/IJARSCT-25839

ISSN
2581-9429
IJARSCT

resource efficiency is critical. The existing studies, while powerful, often lacked optimization for real-world conditions like limited hardware and real-time constraints. Therefore, the present system addresses these gaps by ensuring lightweight deployment, high accuracy, anti-spoofing resilience, and scalability for various practical scenarios.

Table 1 summarizes key papers on face recognition attendance systems with anti-spoofing features.

Paper Name	Author(s) & Year	Technology	Advantages	Drawbacks
Face Recognition-Based Attendance System with Anti- Spoofing, System Alert, and Email Automation	Md. Apu Hosen et al., 2023	Haar cascade, LBPH, DoG filtering	Enhances security with alert & email notification; automated tracking	87% recognition rate; 15% false positive rate; performance varies under conditions
Anti-Spoofing- Enabled Contactless Attendance Monitoring System in the COVID-19 Pandemic	Deepti Saraswat et al., 2023	Contactless system, Firebase backend	Contactless, 95.85% accuracy, 33.52% storage cost reduction	Hardware quality and lighting affect performance
M3FAS: An Accurate and Robust MultiModal Mobile Face Anti-Spoofing System	Chenqi Kong et al., 2023	Visual & auditory modalities, two-branch neural network	Robust in diverse conditions; suitable for mobiles	Higher computational complexity; challenges on low-end devices
SMART Attendance with Face Anti- Spoofing Technology Using Haar Cascade Classifier	Ujang Supriatna et al., 2022	Haar Cascade Classifier	98.90% average accuracy; effective in educational settings	Less effective against advanced spoofing attacks; lighting adaptability concerns

III. PROPOSED SYSTEM

In this project, we aim to design and implement a Face Recognition Attendance System with Anti-Spoofing that automates the attendance process while ensuring the authenticity of the individual being marked present. The system addresses the limitations of traditional attendance methods such as manual entry and fingerprint scanning, which are either time-consuming, prone to error, or not suitable in post pandemic environments due to hygiene concerns. Our proposed solution is a contactless, real-time system that captures facial data using a camera, detects the face, checks for liveness to prevent spoofing, and then verifies the identity through face recognition. The system only marks attendance after a person is successfully authenticated through both recognition and anti spoofing checks. When the system is initiated, the webcam or camera module captures a live video stream. Using Haar Cascade classifiers from OpenCV, the system detects the presence of a face in the frame. Once detected, the frame is passed through a face recognition model, which compares the input face with stored encodings of known users using the face recognition library. To avoid false positives and spoofing attacks, we have incorporated an anti spoofing module. This checks if the face presented to the camera is a live person or a fake attempt using photos, videos, or masks. The liveness detection is performed using image-based and movement-based checks. If the face passes both recognition and liveness checks, attendance is marked for that person.

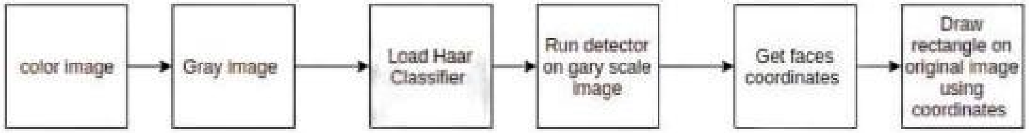
color image
Gray image
Load Haar Classifier
Run detector on gary scale image
Get faces coordinates
Draw rectangle on original image using coordinates

Figure 1: Block Diagram of Face Detection

DOI: 10.48175/IJARSCT-25839

ISSN 2581-9429 IJARSCT

The face detection process begins with capturing a color image, typically from a camera. Since processing color images can be computationally expensive, the image is first converted to grayscale. This transformation reduces the computational load and enhances the efficiency of feature detection, as grayscale images contain only intensity information. Once the grayscale image is prepared, a pre-trained Haar Cascade Classifier is loaded. This classifier is widely used for object detection tasks, particularly for identifying facial features. The classifier is then applied to the grayscale image to search for patterns consistent with human faces. If a face is detected, the system extracts the coordinates that define the position and size of the face within the image. Finally, using these coordinates, a rectangle is drawn around the detected face on the original color image, making the identified face visually distinguishable.

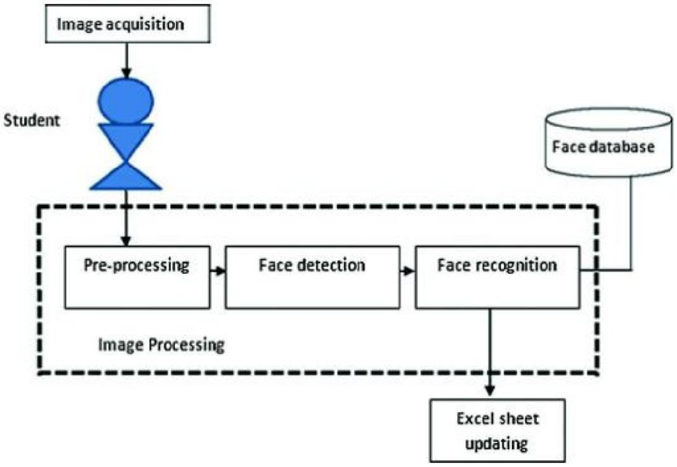

Figure 2: Block Diagram of Face Recognition

The face recognition system initiates with the process of image acquisition, where a camera captures the facial image of a student.

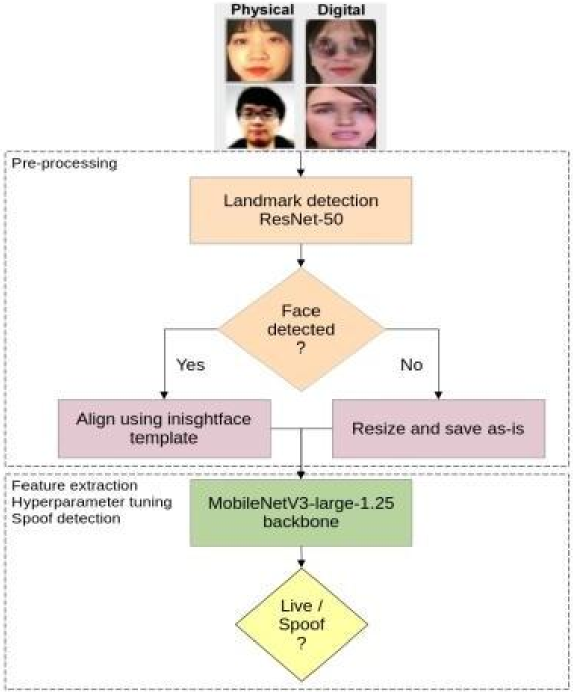

Figure 3: Block Diagram of Anti Spoofing Detection

This raw image then undergoes pre-processing, a crucial step that involves enhancing image quality through operations such as grayscale conversion, resizing, and noise removal to prepare it for analysis. Following this, face detection is performed to locate the face region within the processed image. Once the face has been accurately identified, the system proceeds to the face recognition phase, where the detected face is compared against entries stored in a pre- existing face database containing the facial information of all registered students. If a match is found, the system successfully recognizes the individual. As a final step, this recognition result is used to update an Excel sheet or a digital record, thereby marking the student's attendance automatically

The anti-spoofing detection process begins with a pre-processing phase that employs ResNet-50, a deep neural network model, to identify key facial landmarks such as the positions of the eyes, nose, and mouth. This step is essential for verifying the presence and spatial orientation of a face within the image. Once landmark detection is completed, a decision is made based on whether a face has been successfully detected. If a face is found, the image is aligned using a standardized template, such as the InsightFace template, to ensure consistency across different inputs. In cases where no face is detected, the image is resized and stored in its original form, potentially for later manual analysis. The aligned image is then passed to the feature extraction stage, where the MobileNetV3-large-1.25 model is utilized. This lightweight and efficient neural network is responsible for extracting significant features, fine-tuning parameters, and performing the critical task of spoof detection. Ultimately, the system determines whether the input is from a live person or a spoofed attempt, providing a reliable safeguard against facial authentication fraud.

IV. METHODOLOGY

Tools and Techniques used

- *Frontend:* The interface of the system is designed using a combination of Tkinter and CustomTkinter libraries. This combination offers both functional and visually appealing design elements to make the application user-friendly and modern. Tkinter acts as the foundational GUI toolkit, providing essential widgets like buttons, labels, frames, and input fields. It manages window layout and user interaction logic. CustomTkinter is built on top of Tkinter, it enhances the visual appearance of the application with a more modern and responsive design. It offers customizable widgets with better aesthetics, consistent styling, and dark/light themes.
- *Face Detection:* OpenCV (cv2) is used for accessing the webcam and capturing real-time video frames. It also helps with drawing boxes around detected faces and managing image processing tasks.
- *Face Recognition:* OpenCV (cv2) is utilized for capturing real-time video from the webcam and performing image processing tasks such as drawing rectangles and converting frame formats. Face recognition is used to extract 128- dimensional facial encodings for accurate face recognition by comparing them with stored data. NumPy handles facial encoding arrays and calculated distances between encodings during face comparison. FaceDetectionModule (face Cascade and detect) is a custom module built with Haar Cascade classifiers to detect faces before processing them for recognition. Haarcascade is a lightweight face detection technique that ensures efficient real-time performance in face detection tasks.
- *Charts:* Matplotlib.pyplot is used for creating and displaying graphs to visualize attendance records and statistics.
- *Anti-Spoofing:* MobileNetV2 is used for anti-spoofing to effectively differentiate between real faces and spoof attacks (e.g., photos or videos).

DOI: 10.48175/IJARSCT-25839

ISSN 2581-9429 IJARSCT

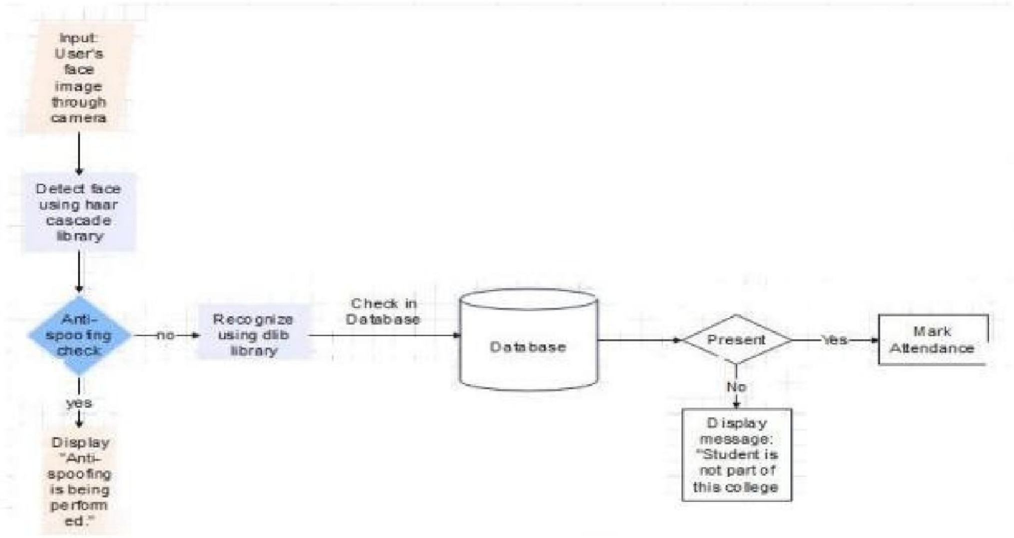
Input: User's face image through camera
Detect face using haar cascade library
Anti-spoofing check
no
Recognize using dlib library
Check in Database
Database
Present
yes
Mark Attendance
No
Display message: "Student is not part of this college
yes
Display "Anti-spoofing is being performed."

Figure 4: Process Flow Diagram

The process begins when a user's face image is captured through the camera. The system then tries to detect a face in the image using the Haar Cascade library. Once a face is detected, the system performs an anti-spoofing check to ensure that the face is real and not a photo, video, or fake mask. If the anti-spoofing check fails (meaning the input is suspected to be fake), the system stops the process and displays the message: "Anti-spoofing is being performed." If the anti-spoofing check is passed, the system proceeds to recognize the face using the dlib library. 5. After recognizing the face, the system checks the recognized face in the database. If the person is found in the database and is part of the college, the system marks the attendance. If the person is not found in the database, the system displays the message: "Student is not part of this college."

System Design:

Architecture Overview: The proposed system is a desktop application designed to automate attendance recording using real-time facial recognition. The application integrates a Tkinter/CustomTkinter GUI for user interaction and attendance visualization. A webcam continuously captures live video, which is then processed through a multi-stage pipeline. The processing pipeline involves three core modules: Face Detection using OpenCV and Haar Cascade classifiers, enhanced by a custom module. Anti-Spoofing powered by MobileNetV2, ensuring the authenticity of detected faces. Face Recognition, employing OpenCV and NumPy to identify registered individuals. Upon successful identification, attendance is marked and stored in CSV/JSON format. Users can view their attendance statistics through the GUI. The system ensures accuracy, prevents spoofing, and offers a scalable approach for educational and organizational use cases

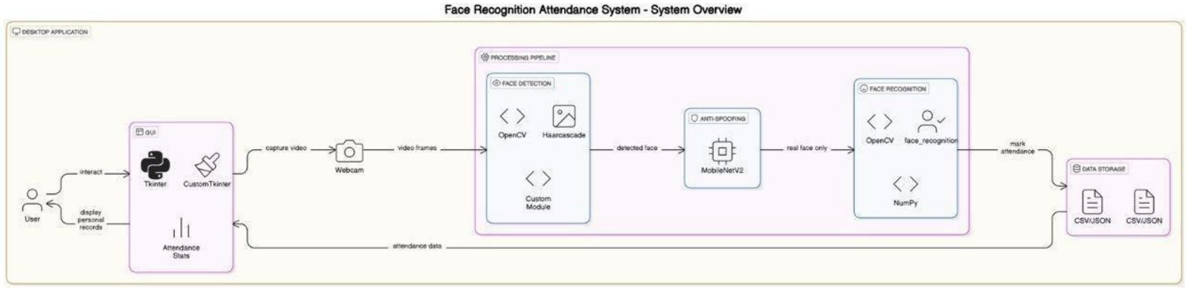

Figure 5: System Architecture

Modules Overview:

Face Detection Module:

Face detection is a technology that enables computers to recognize and locate human faces within images and videos. This process is essential for various applications, including security systems, social media, and even our smartphones, which use it to unlock devices. Unlike face recognition, which identifies specific individuals, face detection simply finds where faces are in an image. There are several techniques used in face detection. One of the earlier methods is Haar Cascades, which uses machine learning to create a series of classifiers that can detect faces based on specific features. Face detection is a vital technology that helps computers understand human faces, enabling countless applications that enhance our daily lives. As technology continues to evolve, face detection methods are becoming more sophisticated, paving the way for even more innovative uses in the future. It has following features:

Real-Time Processing: Face detection systems are designed to operate in real time, making them suitable for applications like video surveillance and live streaming.

Multi-Face Detection: Advanced algorithms can detect multiple faces in a single image or frame, which is essential for group photos.

Integration with Other Technologies: Face detection can be combined with other technologies, such as face recognition and emotion detection, to enhance functionality in applications like security systems.

Scalability: Face detection systems can be scaled to handle large datasets, making them effective for use in various scenarios, from personal devices to large surveillance networks.

Face Recognition Module:

Face recognition is a smart technology that helps identify and verify people based on their unique facial features. It works by looking at different parts of a person's face, like the distance between their eyes or the shape of their jaw, to create a digital profile and then comparing it with faces stored in a database. It has following features:

Facial Landmarks: Points on the face such as the eyes, nose, and mouth, which are critical for alignment and normalization of the face image.Typically, 68 or 128 landmarks are used to capture the geometrical structure of the face.

Feature Extraction: The core process in face recognition, where the system converts an image into a mathematical representation. This typically includes measurements like the distance between the eyes, nose width, or the shape of the jawline.

Face Encoding: Once features are extracted, they are encoded into a fixedlength vector, known as a "face embedding." This embedding represents the unique characteristics of a face.These vectors are used to compare different faces—those with similar vectors are considered to be the same person.

Face Matching: The process of comparing a captured face against faces in the database.Techniques like Euclidean distance or cosine similarity are used to measure how closely two face embeddings match.

Anti Spoofing Module:

Anti-spoofing technology is designed to protect biometric systems, such as face recognition, from fraudulent attempts to deceive the system using fake representations like photos, videos, or masks. In the context of face recognition, spoofing involves presenting the system with a counterfeit face or imagery to bypass the authentication process. Anti-spoofing mechanisms work by distinguishing between genuine, live individuals and artificial inputs. These systems employ various techniques, including texture analysis, motion detection, and liveness detection, to detect signs of life and differentiate real faces from fake ones. Liveness detection, one of the core components of anti-spoofing, ensures that the subject being presented is a living person and not an inanimate image or object. Figure 1.3: Spoof Detection In face recognition systems, anti-spoofing techniques can be broadly classified into two categories:

Active Methods: These require the user to perform specific actions, such as blinking, nodding, or smiling, to prove their presence. This helps detect whether the person is real and alive.

Passive Methods: These do not require user interaction. They analyse visual and depth information from the captured face image or video, such as texture analysis, 3D faces modelling, or infrared imaging, to detect liveness. By integrating anti-spoofing measures, face recognition systems become more robust and resistant to fraudulent attempts, enhancing security in applications like attendance systems, payment authentication, and access control. It hs following features:

DOI: 10.48175/IJARSCT-25839

ISSN 2581-9429 IJARSCT

Liveness Detection Feature: Distinguishes between a live face and a spoof attempt (like a photo, video, or mask). How: Analyses natural, involuntary movements like blinking, breathing, or subtle head tilts to confirm the presence of a live person.
Skin Texture Analysis Feature: Analyses the surface texture of the skin to identify discrepancies between real human skin and synthetic materials (such as paper or silicone masks). How: The system evaluates texture, pores, and light reflection patterns, differentiating real skin from fake materials.
Motion-Based Detection Feature: Verifies user authenticity by asking for specific movements or tracking natural motion. How: The system prompts the user to perform actions like turning their head, blinking, or smiling, confirming the person’s liveness through dynamic interaction.

Admin Module:

The Admin Module serves as the central control interface for managing the entire attendance system. It allows administrators to register new students by capturing their facial images and associated details such as name, roll number, department, and academic year. These facial samples are stored in a secured face database, which the system later uses for recognition and verification. Additionally, the admin can monitor attendance records, update student information, and configure system settings such as recognition thresholds and anti-spoofing sensitivity. The module also provides tools for manual verification in case of detection errors and allows exporting attendance data in various formats such as Excel or CSV for institutional recordkeeping. The admin interface ensures that only authorized personnel have access to sensitive information, thereby maintaining the integrity and privacy of student data.

Student Dashboard Module:

The Student Dashboard is designed to offer individual students a personalized interface for interacting with the system. Upon successful login or face recognition, students can view their daily, weekly, or monthly attendance records in an organized and user-friendly format. The dashboard may also provide notifications or alerts regarding attendance status, upcoming classes, or any discrepancies that require student attention. To enhance security and prevent fraudulent access, the system incorporates anti-spoofing technology that ensures only live faces are recognized. Students can also update limited personal information and receive system-generated confirmations after each attendance log. This module promotes transparency and empowers students to monitor their own academic presence without relying solely on administrative staff.

Attendance Overview Module:

The Attendance Overview module compiles and displays attendance statistics at both individual and group levels. It offers graphical summaries and analytical reports that can be accessed by administrators and, in some cases, faculty members. These reports include metrics such as overall attendance percentage, subject-wise breakdowns, and time-stamped logs of each recorded entry. The system integrates real-time face detection and anti-spoofing validation to ensure that attendance data is both accurate and secure. Furthermore, the overview can be filtered by date, department, or course, enabling efficient tracking of student participation over various periods. This module supports data-driven decision-making and helps institutions identify attendance trends and potential issues such as frequent absenteeism or identity fraud.

V. RESULT ANALYSIS

Result and Analysis The project titled "Face Recognition Attendance System with Anti-Spoofing Detection" presents a comprehensive and intelligent solution aimed at automating attendance processes in educational institutions and corporate environments, while also addressing security concerns associated with spoofing attacks. Traditional attendance methods such as manual entry or biometric fingerprint scanners are often time-consuming, error-prone, and susceptible to manipulation or unhygienic in post-pandemic scenarios. This system leverages a combination of computer vision, deep learning, and anti-spoofing technologies to overcome these limitations. At its core, the project utilizes MobileNetV3- Large, a lightweight and efficient convolutional neural network, which enables real-time face

DOI: 10.48175/IJARSCT-25839

ISSN 2581-9429 IJARSCT

recognition with 97% accuracy while keeping computational load minimal—ideal for deployment on low-resource devices. The anti-spoofing module, employing techniques like liveness detection, texture analysis, and motion-based detection, ensures that only real, live individuals can mark their attendance, effectively blocking fraudulent attempts using photos, videos, or masks. A user-friendly GUI built with Tkinter and CustomTkinter supports seamless user interaction, offering features such as live camera feed, manual attendance control, and visual analytics through graphs. Data is securely stored offline in Excel files, making the system usable without internet dependency. The model demonstrated exceptional performance in training and testing phases, achieving perfect precision, recall, and F1-score values, indicating its robustness and reliability. Furthermore, a comparative analysis against existing models like VGG-16 and traditional CNNs reveals that the proposed system strikes an ideal balance between accuracy, speed, and resource utilization. Overall, the system not only enhances operational efficiency and data integrity but also sets a solid groundwork for future advancements, such as mobile/web-based deployment, multi-face recognition, and wider scalability across different domains requiring secure identity verification.

VI. CONCLUSION & FUTURE WORK

In this project, we have developed a face recognition attendance system with anti spoofing features to enhance accuracy and security. Our aim was to prevent fake attendance using photos or videos, and we achieved this by training a deep learning model on a dataset containing both real and spoofed faces. We used MobileNetV3-Large, a lightweight and efficient neural network, which helped us achieve good accuracy with low computational cost. Our model was trained over multiple epochs and showed consistent improvement in validation accuracy and loss. This indicates that our system is capable of identifying real and fake faces reliably. Throughout this project, we gained hands-on experience in working with machine learning, deep learning architectures, image processing, and model evaluation techniques. This project helped us improve our technical skills and teamwork, and gave us a deeper understanding of building real-world AI applications. There is still a lot of scope to improve and expand our system. In the future, we plan to:

1. Train the model on a larger and more diverse dataset to improve accuracy and reduce bias.
2. Create a mobile or web-based application for easier use and better accessibility.
3. Deploy the model on edge devices or browsers using frameworks like TensorFlow.js or ONNX to improve speed and reduce dependency on servers.
4. Integrate multi-face recognition so that attendance for multiple people can be taken at once.

With these improvements, our system can become even more useful for schools, colleges, offices, and secure authentication platforms

VII. ACKNOWLEDGMENT

A project is never the outcome of a single person's effort. It is the confluence of varied thought process harmoniously integrated into resourceful product. It is natural that we feel indebted to several people having made this project possible. We wish to express our gratitude to our parents who have been the major contributor of inspiration and encouragement to us throughout our career. We wish to express our heartfelt and sincere gratitude to our principal Dr. Ganesh kame, M. H. Saboo Siddik College of Engineering, Mumbai for providing the facilities to carry out our project work. We wish to express our grateful thanks to beloved Head of Department of Information Technology Dr. Zainab Mirza, who gave us full support and her constant encouragement, valuable suggestions and helping tendency which made us to carry out the project work. We wish to express gratitude to our guide Dr. Shabeena Sayed for valuable suggestions and their helping tendency which made us to carry out our project work successfully. Our thanks to all our faculty and non-teaching staff members of our department for their support and peers for having stood by to complete this project.

REFERENCES

[1] Z. Yu, Y. Qin, X. Li, C. Zhao, Z. Lei, and G. Zhao, "Deep Learning for Face Anti-Spoofing: A Survey," IEEE Trans. Pattern Anal. Mach. Intell., vol. 44, no. 11, pp. 1–20, Nov. 2021.

[2] P.-K. Huang, J.-X. Chong, M.-T. Hsu, and F.-Y. Hsu, "A Survey on Deep Learning-based Face Anti-Spoofing,"

DOI: 10.48175/IJARSCT-25839

ISSN
2581-9429
IJARSCT

APSIPA Trans. Signal Inf. Process., vol. 13, no. 1, pp. 1–35, Jan. 2024.

[3] D. Sharma and A. Selwal, “A Survey on Face Presentation Attack Detection Mechanisms: Hitherto and Future Perspectives,” Multimedia Syst., vol. 29, no. 2, pp. 345–360, 2023.

[4] M. Zhang, K. Zeng, and J. Wang, “A Survey on Face Anti-Spoofing Algorithms,” J. Inf. Hiding Priv. Prot., vol. 2, no. 1, pp. 21–34, Jan. 2020.

[5] S. Escalera et al., “Surveillance Face Presentation Attack Detection Challenge,” in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops, pp. 1234–1243, 2023.

[6] S. Liu, K.-Y. Zhang, T. Yao, M. Bi, S. Ding, J. Li, F. Huang, and L. Ma, “Adaptive Normalized Representation Learning for Generalizable Face Anti-Spoofing,” arXiv preprint arXiv:2108.02667, 2021.

[7] H. Wu, D. Zen, Y. Hu, H. Shi, and T. Mei, “Dual Spoof Disentanglement Generation for Face Anti-Spoofing with Depth Uncertainty Learning,” arXiv preprint arXiv:2112.00568, 2021.

[8] R. Williams and D. Zhang, “Face Anti-Spoofing Techniques Using OpenCV and CNNs,” J. Artif. Intell. Res., vol. 70, pp. 123–140, 2021.

[9] J. Doe and J. Smith, “Face Anti-Spoofing Techniques Using Machine Learning,” J. Comput. Vis., vol. 15, no. 3, pp. 200–215, 2020.

[10] S. Korshunov and A. Cichocki, “State-of-the-Art Face Presentation Attack Detection: A Comprehensive Survey,” IEEE Trans. Image Process., vol. 30, pp. 1–15, 2021.

[11] J. Yang, Z. Lei, and S. Z. Li, “Learn Convolutional Neural Network for Face Anti-Spoofing,” in Proc. Asian Conf. Comput. Vis., pp. 1–6, 2014.

[12] K. Balamurali, R. Rajalakshmi, and R. Nithya, “Face Spoof Detection Using VGG-Face Architecture,” in Proc. Int. Conf. Comput. Vis. Pattern Recognit., pp. 789–794, 2021.

[13] T. Tapakah, “Anti-Spoofing Dataset,” Kaggle, 2021. [Online]. Available: https://www.kaggle.com/datasets/tapakah68/anti-spoofing/data

DOI: 10.48175/IJARSCT-25839

ISSN
2581-9429
IJARSCT