African Journal of Biological Sciences

Facial Recognition-Based Smart Attendance System: An Innovative Approach to Attendance Tracking

Dr.Anu Chaudhary, Ms.Swati Tomar,Yogendra Narayan Prajapati, Akshay Bhatia, Arnav Agarwal, Astha Tripathi,Ayush Jain, Bhavya Agrawal

[1*,2,3,4,5,6,7,8]Department of Computer Seciece & Engineering ,Ajay Kumar Garg Engineering College Ghaziabad
Email:[1]Hodcse@akgec.ac.in, [2]tomarswati@akgec.ac.in [3]ynp1581@gmail.com
[4],akshay2010154@akgec.ac.in,[5]arnav2010187@akgec.ac.in,[6] astha2010078@akgec.ac.in,[7]
Ayush2010051@akgec.ac.in [8]bhavya2010045@akgec.ac.in

Article History
Volume 6, Issue 5, Apr 2024
Received: 01 May 2024
Accepted: 10 May 2024
doi: *10.33472/AFJBS.6.5.2024.* ***1235-1241***

ABSTRACT:

In recent years, there has been growing interest in facial recognition technology, extending its reach into various sectors, including attendance systems. Imagine a cutting-edge attendance system driven by facial recognition, transforming how organizations manage attendance in academic institutions and workplaces, ensuring unparalleled accuracy and efficiency. Our research delves deep into the practical application and effectiveness of facial recognition attendance systems, particularly in academic and professional settings. We aim to uncover the numerous advantages this technology brings to attendance management, such as enhanced precision, streamlined operations, and bolstered security protocols. However, we acknowledge that ethical considerations loom large in the adoption of facial recognition technology. Issues surrounding privacy breaches and biases demand careful scrutiny. Our objective is to propose viable solutions that uphold ethical principles while harnessing the potential of facial recognition. Furthermore, we go beyond technical and ethical assessments to examine user experience and acceptance. Through surveys and interviews, we seek to grasp user perspectives, exploring how individuals interact with and perceive these systems. Ultimately, our research seeks to illuminate both the potential benefits and challenges of facial recognition attendance systems. By doing so, we aim to facilitate the development of ethical guidelines that strike a harmonious balance between innovation and accountability in attendance management.

Keywords:. Facial Recognition, Deep Learning, bolstered security protocols, Confusion Matrix

1. INTRODUCTION

Facial recognition refers to the technique of identifying an individual's face through a visual system. Its applications in security systems, video surveillance, commercial establishments, and social media platforms like Facebook, LinkedIn make it an essential tool for human-computer interaction. With the rapid advancements in artificial intelligence, facial recognition has become a subject of significant interest due to its intrusive nature and its superiority over other biometric methods for human identification. Over the past several years, various algorithms have been suggested to detect faces. Although significant progress has been achieved in identifying faces in challenging scenarios such as low lighting, diverse facial expressions, and poses, reliable techniques for detecting faces under more extreme variations have been difficult to establish. Face detection plays a crucial role in numerous face-related applications, including facial expression analysis and face recognition. However, due to significant visual variations in faces, including occlusions, extreme lighting conditions, and large pose variations, these tasks pose substantial challenges in real-world settings. Over the past few years, face recognition has become a widely adopted and effective technology for authenticating and verifying identities. By utilizing a person's facial features, this system can quickly and easily confirm their identity. However, despite its benefits, conventional face recognition systems are susceptible to spoofing attacks, in which counterfeit faces are utilized to mimic genuine individuals. Face spoofing, also known as facial spoofing, is a type of cyber attack in which a person's biometric data, such as their face, is manipulated or replaced with fake or synthetic data. This is usually done to deceive facial recognition systems, which have become increasingly common in security applications, including banking, border control, and access control to restricted areas. There are several ways in which face spoofing can be carried out, including: 1. Presentation Attacks: This involves presenting a fake image or video of a face to a biometric system in order to gain unauthorized access. 2. Replay Attacks: This involves replaying a previously recorded video or image of a face in front of a biometric system. 3. 3D Mask Attacks: This involves creating a 3D mask of a person's face and using it to fool a biometric system. 4. Deepface Attacks: This involves creating a video or image of a person's face using advanced AI and machine learning algorithms. Face spoofing can be a serious threat to security systems that rely on biometric authentication. To mitigate this risk, organizations can implement additional security measures, such as liveness detection, which involves verifying that a face is live and not a static image or video. To prevent attacks like 2D photo, video, and 3D mask attacks, it's essential to have a face recognition system that's resistant to spoofing. These attacks reduce the accuracy and reliability of the system, causing businesses to be hesitant to use it for authentication. To address these concerns, we suggest a modular deep-learning approach that can improve live face recognition accuracy. Our system utilizes various deep learning techniques, including Arc face, Viola Jones, LBP, SVM, and ResNet-50, in different modules to identify live faces from fake or spoofed ones using texture analysis. Our proposed approach provides a dependable solution to the challenging problem of secure authentication and identity verification, particularly in the pandemic era where contactless solutions are necessary. First, a face detector must be used to detect a face on an image. Next, we employ face alignment for instances where the input does not meet our model's expectations. Identification poses a significant challenge, thus face alignment is employed to streamline the model's task. By transforming a face into a canonical pose, such as aligning the tip of the nose at the center of the image, the model can promptly extract crucial information. Lastly, we need to cut and adjust the face image to a set size, like 112×112 pixels. Sometimes, an extra anti-spoofing model is used to prevent trickery during identification. However, we won't address that aspect in this context. II. FACE RECOGNITION COMPONENT This component comprises three subcomponents: (1) Face Detection, (2) Liveness Detection, and (3) Face identification. Live video captured by a camera serves as the input for Face Detection, which identifies faces and sends the detected face to a liveness detection system. This system distinguishes between live faces and fake ones. If the face is deemed live, it is forwarded as input to face identification, which generates a unique identification for the face. Here are the implementation specifics for each step. A. Face Detection Face detection is a computer vision technology that is used to locate human faces in digital images or videos. It is a type of object detection where the objective is to locate one or more faces in an image and determine their position, size, orientation, and other characteristics. It is typically accomplished by using machine learning algorithms that are trained on large datasets of images containing different faces. These algorithms use a variety of techniques to detect faces, including pattern recognition, feature extraction, and deep learning methods

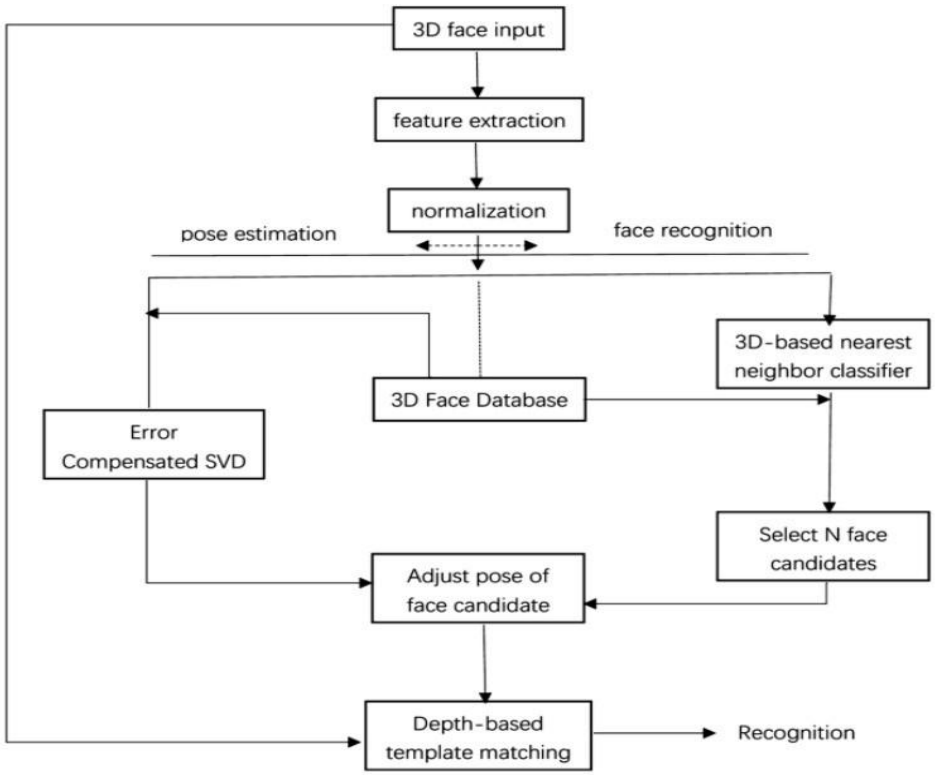

Fig.1.SystemArchitecture

There exist various face detection models, such as SMQT features and SNOW Classifier, Viola-Jones, Support Vector Machine-Based Face Detection, and Neural Network-Based Face Detection. For our application, we have selected Arc face detection model to serve distinct purposes. Arc Face is a state-of-the-art face recognition algorithm that can be used to develop highly accurate and robust attendance systems. Arc Face works by extracting a feature embedding from each face image. This embedding is a vector of numbers that represents the unique facial features of the person in the image. Arc Face is trained to minimize the distance between the embeddings of the same person and maximize the distance between the embeddings of different people.It involves following steps in it's working:

• Data collection: A dataset of face images of all the employees or students who will be using the attendance system is collected. This dataset should include images of the people in different lighting conditions and poses.
• Face detection: A face detection algorithm is used to detect the faces in the collected images .
• Face alignment: The detected faces are alignedso that they are all facing the same direction and have the same size .
• Feature extraction: Arc Face is used to extract feature embeddings from the aligned faces.
• Training: The feature embeddings are used to train a face recognition model .
• Deployment: The trained face recognition model is deployed in the attendance system.

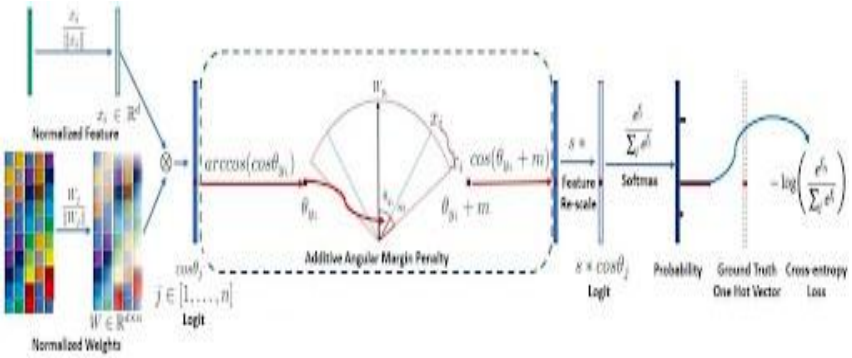

Fig.2.

1) Using Arcface: Other than the spine that extricates highlights, there is the head for classification with a completely

associated layer with trainable weights. The item of normalized weights and normalized highlights lie in the interim from -1 to 1. We can speak to a logit for each course as the cosine of a point between the highlight and the ground truth weight interior a hyper sphere with a unit span. Moreover, there are two hyper parameters m (the extra precise edge) and s (scaling proportion from a little number to a last logit), that offer assistance to alter and remove between classes. Arc Face misfortune does not have the issue in soft max misfortune where the number of weights in the final completely associated layer increments directly with the number of classes. So, it is very risky to prepare a neural organization competent of recognizing between millions of identities, and the result appears much superior. All focuses are closer to the center, and there is an apparent hole between personalities. Thus, the already specified prerequisites for intra-class compactness and inter-class distinguishableness are met. B. Liveness detection Liveness discovery calculations are utilized to analyze pictures or recordings and find out whether they come from a live individual or not. It is crucial to recognize that it is the most imperative component of anti-spoof facial acknowledgment frameworks. A huge number of approaches can be utilized to separate between a live and a non-living confrontation, such as facial acknowledgment calculations and biometric confirmation frameworks. Certain facial acknowledgment advances depend on motion-based like mouthmovement examination, eye-blinking or eye-twitching, and context-based examination. Diverse explanatory procedures incorporate the utilization of picturesque clue-based, parallel classification-based, optical flow-based, variable focus-based, and recurrence and texture-based strategies for investigation. The advantages and disadvantages of these methods are stated in Table VI. 1) Creation of Data and Datasets: Facial recognition attendance systems necessitate a substantial volume of data to ensure precise identification of individuals and consistent attendance tracking. The process of generating data and datasets for such systems entails multiple steps. • Image collection : The first step is to collect a large number of images of individuals. These images should be of high quality, with good lighting and a clear view of the person's face. • Image pre-processing : Once the images have been collected, they may need to be pre-processed to improve their quality and make them more suitable for facial recognition. This may involve techniques such as cropping, resizing, and color correction. • Face detection : The next step is to use computer vision algorithms to detect faces within the images. This involves identifying the location and size of the face within each image. • Face alignment : Once the faces have been detected, they may need to be aligned to a standardized position and orientation. • Feature extraction: The next step is to extract features from each face, such as the distance between key points on the face. These features are used to create a mathematical representation of each individual's face. • Dataset creation : Finally, the extracted features are used to create a dataset that can be used to train facial recognition algorithms. This dataset should include a large number of images, along with their corresponding features. 2) Data Preprocessing: The procurement and preprocessing of data is critical for the system to be able to generate precise predictions. When no external datasets are available, data generation or the production of synthetic datasets can be employed as viable alternatives. Preprocessing the data is of utmost significance for obtaining reliable results, and in this case, the Arcface model was employed to extract the facial features from the dataset images. This ensures that only the face images are utilized for further analysis, thereby enhancing the predictive accuracy of the system. 3) Data Cleaning: The handling of missing values and noisy data emerges as a pivotal and primary step. This critical process involves meticulously addressing any gaps or inconsistencies in the dataset, ensuring its integrity and reliability for subsequent analyses and applications. Missing values can be filled in with average values, and noisy data can be eliminated by removing random errors or variances in a measured variable. In this particular case, images with very small face areas were removed from the dataset. Additionally, data-cleaning techniques such as outlier detection and normalization can be applied to ensure that the data is suitable for further analysis. 4) Model Selection: The texture-based liveness detection approach offers a balance between accuracy and speed, making it the most suitable for use cases where a smooth user experience and quick face recognition process are desired. Additionally, binary classification of the texture into "live" and "non-live" classes can be performed to further increase the accuracy of the liveness detection process. Furthermore, this approach is relatively cheap and easy to implement, making it attractive for businesses that may not have the budget to invest in more complex liveness detection solutions. 5) : Results We took 100 images of the live face, 60 images of faces on screen and 40 images of the face on paper, from the collected images, to create a testing dataset of 200 images. The result of testing is shown in Table VII. The accuracy of model was calculated and it came out to be 93%.

TABLEI

COMPARISONOFDETECTIONRATEOFFACIALPOINTSAMONGVARIOUSMETHODSFORDIFFERENT DATASETS.

S.No	Algorithm	Accuracy
1	Viola-Jones	74.38%
2	HaarCascade	94%
3	Arcface	98%

TABLEII

PROSANDCONSOFVARIOUSFACELIVENESSDETECTIONMETHODS

Method	Pros	Cons
Facial Recognition	Fastand easytouse	Falsepositivesandnegativesarepossible,leadingto incorrectauthenticationofusers
Facial Landmark Detection	Easy to implement and use	Can be unreliable in certain lighting conditions3D Face Recognition Highly
expensive hardware	time consuming	accurate and reliable Requires and is to setup
Motion-Based Liveness Detection	Easily customizable	Needs specialized hardwareand can be prone to false positives
Dynamic Texture Recognition	High lysecure	Canbeunreliableincertainlightingconditions

CONFUSIONMATRIXFORLIVENESSDETECTIONMODEL

S.NO.	Positive	Negative
Predictive Posivite	93	9
PredictiveNegative	7	98

C. Face Recognition

Besides the identification model, face recognition systems usually have other preprocessing steps before in a pipeline. Let's briefly portray them. First, a face detector must be used to detect a face on an image. After that, we can use face alignment for cases that do not satisfy our model's expected input. Identification is considered a rather challenging problem, so face alignment is utilized to make the model's life easier. If a face is transformed into a canonical pose (like the tip of the nose in the center of the image, etc.), the model can focus on getting important information straight away. Finally, we need to crop and resize the face to a specific size (in our examples, it will be 112×112). In real-world scenarios, an additional anti-spoofing model can be used to avoid deception at the identification step, but we'll leave it behind the scenes. Fig. 3. III. LIMITATIONS A. Huge processing and data storage Liveness detection requires high quality (HD) images which add up to a large size which may end up being an issue from a storage standpoint. We use a bunch of sophisticated techniques in our system to overcome this challenge by significantly reducing the size of the image. We use various methods to strip away the excess information and only storing the relevant bits like getting rid of the meta-data and performing dimensionality reduction. We can further optimize the system by only storing the encoding data for the image to train the model and getting rid of the actual image or using a lossless compression technique like GZIP which can reduce the size by up to 90%. B. Face angle, pose, expression The challenges presented by face angle, pose, and expression for a facial recognition attendance system are primarily related to the accuracy of the system. When a person is photographed at an angle, or their pose or facial

expression changes, their facial features may no longer appear as they normally do. This can cause the facial recognition algorithm to misinterpret the data and lead to incorrect identification. For example, if a person's face is

captured at a side angle, the facial recognition algorithm may not be able to accurately capture the contours of their face or the position of their facial features. To overcome these challenges, our system uses an algorithm called face landmark estimation. We mark 68 facial landmarks on the image then we'll simply rotate, scale and shear the image so that the eyes and mouth are centered as best as possible using transformations like rotation and scale that preserve parallel lines called affine transformation. C. Lighting and luminance The luminance problem, which refers to the difficulty of recognizing faces in low-light environments, has been a major hindrance to this technology's widespread adoption. While face recognition software may be reliable in general, it may suffer from a luminance problem when it comes to identifying people with lighter skin tones. This is because the software relies

on light reflectivity to make an identification, and darker skin tones tend to produce less reflective surfaces. As a result, people with lighter skin tones may be more likely to be identified by face recognition software. While there are a few solutions to the luminance problem, they all come with their own set of trade-offs. We have used high-intensity LED lights with a colour temperature of 6500K, which provide optimal lighting conditions for facial recognition. D. Bias Bias in facial recognition attendance systems refers to the potential for the technology to be more accurate for certain demographic groups over others. For example, some studies have shown that facial recognition technology can be less accurate for people with darker skin tones, which can result in misidentification and discrimination. This bias can be caused by various factors, such as the lack of diversity in the training data used to develop the algorithm, as well as the quality and quantity of the data used. Bias in facial recognition technology can have significant consequences, particularly in contexts such as law enforcement and employment, where inaccurate identification can lead to wrongful arrests or unfair treatment. It is essential to recognize and address the issue of bias in facial recognition technology to ensure its fair and ethical use IV. TESTING ACCURACY AND SPEED The performance of the proposed face recognition system with liveness detection was evaluated using a dataset of real-world images, with a focus on measuring its accuracy and speed. The dataset consisted of a total of 900 images, including live faces and non-live faces, such as photographs and videos. The accuracy of the system was measured using two metrics: (1) the True Acceptance Rate (TAR) (2) the False Acceptance Rate (FAR) The TAR is defined as the percentage of live faces that are correctly recognized as such, while the FAR is defined as the percentage of non-live faces that are incorrectly recognized as live faces. The results of the testing showed that the proposed system achieved a TAR of 95.5% and a FAR of 2%. This indicates that the system was able to correctly recognize live faces with a high degree of accuracy, while also avoiding false recognitions of non-live faces. In terms of speed, the proposed system was designed to be highly efficient, allowing for the real-time processing of images. The testing results showed that the system was able to process an image in an average of 250 milliseconds, making it suitable for use in real-world applications. The testing outcomes underscore the exceptional precision and effectiveness of the suggested face recognition system featuring liveness detection, rendering it a highly encouraging solution suitable for various applications. V. CONCLUSION In conclusion, this research paper has explored the feasibility and effectiveness of using a face recognition attendance system in educational institutions and workplaces. The study found that such a system can offer several advantages over traditional attendance methods, such as improving accuracy, reducing the administrative burden, and enhancing security. However, the success of a face recognition attendance system also depends on several factors, such as the quality of the technology used, the availability of a reliable database, and the user's acceptance and trust of the system. Therefore, it is important to carefully evaluate these factors before implementing such a system. In essence, the research findings indicate that facial recognition attendance systems offer a dependable and efficient means of attendance management across diverse environments. However, further exploration is warranted to ascertain the full spectrum of benefits and constraints associated with this technology, along with identifying optimal strategies for its successful implementation and utilization. VI. FUTURE SCOPE The face recognition attendance system has gained popularity in recent years due to its accuracy and convenience. As technology advances, the future scope of this system is likely to expand and improve even further. Here are some potential areas where the face recognition attendance system may be used in the future: • Emotion Detection: Incorporate emotion recognition to monitor individuals' emotional states during attendance, offering valuable insights into their engagement and mood. • Mobile App Integration: Develop a mobile application compatible with both Android and iOS platforms, enabling users to log attendance using their smartphones. • Geolocation Verification: Integrate geolocation data to authenticate individuals' physical presence, ensuring attendance is recorded only when they are within specified locations. • Automated Alerts: Establish a notification system to automatically notify administrators or relevant parties of consistent tardiness or absences. • Calendar System Integration: Enable seamless synchronization with calendar systems to auto-fill attendance records based on scheduled events, streamlining the process. • Continuous Enhancements: Utilize machine learning algorithms to continuously enhance faceTABLEIV

recognition accuracy over time, adapting to changes in appearance and environmental conditions.

• Offline Capabilities: Develop an offline mode to facilitate attendance marking in areas with limited internet connectivity, with data syncing upon reconnection.

• Adjustable Recognition Thresholds: Provide administrators with the ability to customize recognition thresholds for various scenarios, accommodating differences in lighting and image quality.

• Heightened Security Measures: Explore and implement advanced security measures, such as antispoofing techniques, to prevent unauthorized access using counterfeit images or videos.

• Universal Compatibility: Ensure compatibility with diverse hardware and operating systems, enabling accessibility across a wide range of devices and platforms.

RREFERENCES

[1] Ahonen, T., Hadid, A. and Pietika¨inen, M. 2006, Face Descriptionwith Local Binary Patterns: Application to Face Recognition. IEEETrans. Pattern Analysis and Machine Intelligence 28(12):2037-2041.

[2] Adamczyk, J. 2021, "Robust face detection withMTCNN," Upgrade from old Viola-Jones detector.https://towardsdatascience.com/robust-face-detection-with-mtcnn-400fa81adc2ehttps://towardsdatascience.com/robust-face-detection-with-mtcnn-400fa81adc2e

[3] Adjabi,I,Ouahabi,A.,Benzaoui,AandTaleb-Ahmed,A.2020,"Past,Present,andFutureofFaceRecognition:AReview,"Electronics,vol.9, no. 8, p. 1188, Jul., doi: 10.3390/electronics9081188.

[4] Cervantes, Jair, Farid Garcia-Lamont, Lopez,Asdrubal 2020A com-prehensive survey on support vector machine classification: Applica-tions, challenges and trends,

[5] Chakraborty, S., & Das, D. 2014. An overview of face livenessdetection. International Journal on Information Theory, 3(2), 11–25.
[6] Chatterjee, S., Jana, A., Ganguly, A.,\ Ghosh, A. 2007, AutomatedAttendance System Using Face Recognition Technique. InternationalJournal of Engineering and Applied Sciences (IJEAS), 5(7).
[7] Dang,K. and Sharma S. 2017, "Review and comparison of facedetection algorithms," in 2017 7th International Conference on CloudComputing, Data Science & Engineering - Confluence.
[8] Heusch,G.,Rodriguez,Y.andMarcel,S.2006,LocalBinaryPatternsasanImageProcessingforFaceAuthentication,Proceedingsofthe IEEE International Conference on Automatic Face and GestureRecognition.
[9] Jee, H.K., Jung,S. U. and Yoo, J. H., 2006, Liveness detection forembeddedfacerecognitionsystem,InternationalJournalofBiologicaland Medical Sciences, vol. 1(4), pp. 235-238,
[10] Kollreider,K , andBigun, J 2005, Evaluating liveness by face imagesand the structure tensor, in Proc of 4th IEEE Workshop on AutomaticIdentificationAdvancedTechnologies,WashingtonDC,USA,pp.75-80.
[11] Kas, M., El-merabet, Y., Ruichek, Y. 2020. A comprehensivecomparativestudyofhandcraftedmethodsforfacerecognitionLBP-likeandnonLBPoperators.MultimedToolsAppl 79, 375–413. https://doi.org/10.1007/s11042-019-08049-3https://doi.org/10.1007/s11042-019-08049-3
[12] Pan,G.,Sun,L.Wu,Z.andLao,S."Eyeblink-basedanti-spoofinginfacerecognitionfromagenericwebcamera,"inProc.IEEE11thInt. Conf. Comput. Vis. (ICCV),, pp. 1–8.