Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Face Recognition with Anti-Spoofing: A Deep Learning-Based Approach for Secure Biometric Authentication

Deepti S, Shreya Singh, Nethra Sri K M, Aishwaryalakshmi G, Ravi N
Department of Information Technology, PSG Polytechnic College Coimbatore, Tamil Nadu, India

ABSTRACT

Face Recognition is a critical biometric authentication technology that depends on contactless and easy identification using readily available digital cameras. Face recognition can be used in Smartphones, access control systems, attendance in companies, Banking, Healthcare, Examinations, Surveillance etc. However, face recognition system implemented only for recognition purposes is vulnerable to attacks. These attacks are called presentation attacks. This included print, photo, replay,3-D mask and digital attacks.

A novel deep learning-based approach for face recognition and face anti-spoofing (presentation attack detection) is proposed here. It is argued that designing the system in a way that 2-Step authentication is performed is optimal. The model includes face detection, preprocessing, anti-spoofing classification, feature extraction, face embeddings comparisons and authentication. Texture, motion, image quality, depth, illumination, and temporal features can be used for presentation attack detection. The Research will leverage convolutional

neural networks to detect spoofing attacks. Existing open-sourced face anti-spoofing databases will be used to design robust models. Accuracy, precision, recall, F1-score, FAR, FRR, and EER will be calculated to evaluate

the performance. In addition, paper will review security, privacy, database dependency, domain generalization, computational costs and emerging presentation attacks. The proposal framework will serve as a foundation for
future research on Multimodal biometrics, Vision transformers, edge AI and Unknown attack detection using the listed databases.

Keywords: *Face Recognition, Face Anti-Spoofing, Presentation Attack Detection, Deep Learning, CNN, Biometric Authentication, Face Embeddings, Liveness Detection, and Computer Vision.*

1. INTRODUCTION

Biometric Authentication is becoming a necessary and mandatory technology. Unlike conventional authentication mechanisms, biometrics uses inherent traits to verify an individual's Identity. Face Recognition biometrics is a feature which can be easily incorporated into the existing authentication systems. The most significant advantage of this feature is contactless authentication and ability to use existing devices like cameras. A conventional face recognition system has three major stages: detection, feature extraction, and comparison. With the advent of deep learning, comparison is no longer a challenge as the system can be trained to extract features from the individual's face and store it as an embedding. Comparison between two faces with embeddings is relatively easy.

However, a face recognition system that is only capable of performing recognition is vulnerable to presentation attacks. A presentation attack (PA) is an attack where the attacker presents a fake biometric trait to fool the sensor. Some of the common presentation attacks that can fool an automated face recognition system is using a printed or electronic photo, 3-D mask or displaying a video on a phone over the sensor. Face PAD aims to detect whether the presented biometric trait is a PA or a live individual. Several conventional approaches have been used to solve the presentation attach detection (PAD) problem. This includes analyzing texture, motion, image quality, frequency domain, and depth information. Another approach is to use multimodal biometric traits like visible, near-infrared and thermal bands. Convolutional Neural Networks (CNN) can solve the PAD problem because they can learn distinctive features that can distinguish between a live and fake biometric sample. The Idea of the proposed system is to decouple face presentation detection from face recognition. In other words, the Camera captures the face of the user who needs to be authenticated and the face detection module detects the location and orientation of the face. The spoofing module checks if the face captured is genuine or not. If the face is recognized, then it proceeds to the face recognition module.

The proposed architecture can be considered two-layer authentication framework. The first layer focuses on determining if the presented face is genuine while the second layer evaluates whether the face belongs to an authorized user. Using this architecture, the designer can work on both layers independently.

2. BACKGROUND AND FUNDAMENTALS

Face recognition refers to the computer vision technology that uses facial information to identify or authenticate users. Most of the face recognition systems use deep neural networks to encode input face images into low-dimension vector also known as embedding. The encoding can be represented as per equation 1:

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

$$f(x) = [e_1, e_2, e_3, \ldots, e_n]$$
Equation 1

Where x is the input face and ei is the weight of a given neuron. During the enrolment process, the face of the legitimate user is captured and then encoded as shown above. The encoded face is then stored as the biometric template for the user. During Authentication, the system compares the encoded face of the input with stored encoded face to determine if they belong to the same person.
For instance, the cosine similarity can be used to compare two encoded faces A and B as shown in equation 2:

$$S(A, B) = (A \cdot B) / (\|A\| \|B\|)$$
Equation 2

If the score is greater than or equal to a threshold value T , the faces are considered similar as should in Equation 3:

$$S(A, B) \geq T$$
Equation 3

Other similarity metrics used in practice include the Euclidean distance.

In conventional face recognition systems, Computer vision features such as Local Binary Patterns (LBP), Histograms of Oriented Gradient (HOG), Haar-Like features, Principal Component Analysis and others were used to train the recognition model. However, these technologies cannot be used effectively in unconstrained environments due to pose variations, facial expression changes, lighting conditions, Camera variations and image resolution differences. Unlike the conventional approach to face recognition, deep learning algorithms can automatically encode facial features without requiring manual feature engineering, Most face recognition system use Convolutional Neural Networks (CNN) to encode input face images into embeddings. These networks use a deep architecture that helps the system learn complex patterns from the input images. Each layer in a CNN encodes different features of an image. For example, the first few layers encode low-level features in the image such as edges and corners while the last few layers encode high-level semantic features. Deep CNNs have been used widely used in most face recognition systems because of the convolutional layers can detect unique and distinguishing features of the input image. The success of the CNNs in Face recognition is primarily attributed to the big data,
GPU acceleration, transfer learning and CNN innovations. The FaceNet algorithm is among the many CNN based approaches used in face recognition. The algorithm has been used to encode input images into embeddings that can be used to compare two faces. FaceNet has been used in most facial authentication systems because it delivers high accuracy in facial comparison.

3. PROBLEM STATEMENT AND OBJECTIVES

Although the face recognition system has been successfully used in various applications, a system that only uses recognition is vulnerable to presentation attacks. For instance, consider a biometric system that stores the facial image of the legitimate user. The attacker can capture or download the image of the legitimate user and present it to the camera instead of swiping the card. If the system is designed to compare the input face with the stored image of the original user, the presentation attach will be successful. This is because the attacker's image will have enough information for the system to successfully complete the authentication. This indicates, that the face recognition system will not be able to answer the questions like "Whose face is this?" But it should ask "Is this a legitimate face presentation?"

The objective of the research is to address this problem by ensuring the authenticity of the input face is determined before proceeding with the recognition phase. Specifically, this study will :

a. Detect faces from images or Video streams
b. Perform preprocessing on facial images to produce model inputs
c. Detect genuineness of biometric presentations and spoofing attacks
d. Recognize legitimate users after validating the input face with anti-spoofing algorithms
e. Investigate protection against printing, replay, screen, mask and digital presentation attacks
f. Design a system capable of processing images in near-real-time
g. Minimize the occurrence of false acceptances due to presentation attacks
h. Evaluate the performance of the system using classification and biometric- security metrics.

4. LITERATURE REVIEW

Face PAD has been extensively researched along with face recognition technology. Earlier approached to solve the PAD problem relied on conventional Computer vision algorithms to describe texture, Image quality and motion features of the input image. However, the current approaches are using deep learning algorithms to extract distinctive features of the input image. A review of the face PAD literature indicates that there is a need for effective methods for securing face recognition systems against presentation attacks. Multiple researchers have investigated the PAD problem using distinguishing features of real and fake biometrics traits. The distinguishing features used in PAD include texture, color, motion, depth, frequency domain and temporal information [1].

Researchers have also leveraged multimodal data such as visible, thermal, and near-infrared imaging to solve the PAD problem. The most established solution to the PAD problem is through CNNs that can learn discriminant features for a given task. A review of Deep Learning for Face Presentation Attack Detection shows the progress made in using CNNs to solve the PAD problem. The paper discusses CNNs' discriminant features learning, supervision strategies, data sets, evaluation protocols, domain generalization, and challenges with unseen presentation attacks [2].

Texture Analysis has been used in multiple studies to solve the PAD problem. For example, there are dissimilarities between human facial skin and printed materials. These differences can be used to distinguish a real face from the fake image. Most of the attacks like print, photo and 3-D masks present similar visual features as a real

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

face. But, the texture features can be leveraged to detect the print attack. The paper proposes a spoofing detection model that uses texture features derived from texture direction and gradient similarity. The approach was tested using the OULU-NPU database and achieved promising results.

Besides detecting texture features of a real face, other approaches have focused on analyzing the motion features of the face. Replay attacks involve capturing video of the legitimate user and replaying in the camera. Similar, display attacks involve displaying the video on television or Phone screen to make the camera to believe that it is capturing the real user's face.
Detecting a replay attack can be achieved by analyzing the motion features such as facial movements and eye movements. Another approach to detecting reply attacks is to analyze the display features of the image. Moiré patterns, screen flickering, and color distortions are additional features of display attacks.

Another approach to solving the PAD problem is using depth features. Unlike a real face, a printed photo has no depth. So, face recognition system can use stereo vision to detect the depth of the input face. Other approached to detecting depth information in a face include using structured light, time-of-flight and infrared sensors.

The OULU-NPU benchmark has played a vital role in establishing a standardizing PAD evaluation protocol. This database can be used to evaluate face PAD performance under different protocols and environmental conditions. In addition, OULU-NPU, other face PAD databases such as CASIA, MSU-Market and CASIA-SURF can be used to evaluate the performance of the spoofing detection model.
The CelebA-Spoof dataset has enabled researchers to leverage a large number of annotated data to train CNNs and achieve promising results. The domain generalization problem is the main limitation of face PAD that has hindered progress in this field. Domain generalization describes the situation where a model performs poorly when deployed in a domain different from the one used to train it. Domain generalization problem occurs when the factors influencing the performance of the face PAD system are not accounted for during model training. The factors affecting the performance of a face PAD system vary, thus limiting the ability of the designer to design an optimal model. Domain generalization is achieved when models are trained on multiple datasets obtained from different domains. Recent developments in Generative Adversarial Networks (GANs) present a bigger challenge in detecting presentation attacks. It has been argued that GANs can generate high-resolution videos that can fool existing face recognition systems. Researchers have raised concerns regarding future attacks since they are more sophisticated and challenging to detect [4].

RESEARCH GAP
Several research gaps exist in face anti-Spoofing:

- Most face PAD systems rely only on the data used to train the model.
- Certain factors such as lighting and camera type have a significant impact on the performance of face PAD systems.
- Attacks such as using realistic masks and digital media present a bigger challenge to RGB cameras.
- Most Deep learning models have high computational cost.

These issues have prompted researchers to develop modular biometric recognition systems that explicitly incorporate face detection, anti-spoofing and recognition modules.

5. TYPES OF SPOOFING ATTACKS

a. Print Attack

A Print attack is printed photo of the target individual
Characteristics of print attacks include:

1. Static facial contents
2. No Natural three dimensional
3. Printing artifacts
4. Paper boundaries
5. Different reflection characteristics
6. Absence of natural facial movement
7. Replay attack

b. Replay Attack

A replay attack is a previously captured image or video. For Example, the attacker can present a video of the real individual via smartphone or tablet.
Reply attack are generally more challenging that simple print attacks, because the display video might include:

1. Eye movement
2. Head movement
3. Facial expressions
4. Natural-looking temporal changes

But screen artifacts can often be used for detection

c. Screen Attack

A screen attack is the target individual on an electronic display
Display technology differences can cause moiré patterns, reflections, Pixel structures, brightness differences and refresh affect.

d. Three-Dimensional Mask Attack

A 3D mask attempts to replicate a fellow person's facial structure. Masks can be made of silicon, latex, plastic, 3D-printed materials, etc. Since the attack includes three-dimensional geometry, simple depth-based approaches may not work.

e. Digital Manipulation

Modern biometrics systems can also encounter digitally manipulated content, including face swapping, synthetic, manipulated photographs and AI generated faces.

6. PROPOSED SYSTEM

The proposed system utilizes a face recognition with a dedicated anti-spoofing step. The Pipeline is
Camera → Face detection → Preprocessing → Anti-Spoofing → Face recognition → Authentication
The Modules are

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

a. Camera
b. Face detection
c. Image Preprocessing
d. Anti-Spoofing
e. Feature extraction
f. Face Recognition
g. Database
h. Authentication decision
i. User Interface

The core security principle is that identity recognition is not performed unless the presentation has passed the anti-spoofing step. If the spoof is detected, the system immediately rejects the authentication. If the real presentation is detected, the system extracts the facial features and compares the resultant embedding with registered templates.

7. SYSTEM ARCHITECTURE AND METHODOLOGY

a. *Camera Input*

Camera supplies the input image or stream. For real-time authentication, it is possible to process multiple frames rather than only a single frame.

b. *Face Detection*

The Face detector locates the facial region within each frame. A detection region can be represented as shown in equation 4

$$B = (x, y, w, h)$$

Equation 4

Where x and y specify the location of the bounding box. w and h represent the width and height of the bounding box.

Possible detection method include:

a) Haar Cascade
b) HOG-Based
c) CNN-based
d) Modern lightweight object-detection networks

c. *Image Processing*

The detected facial region is normalized for the deep learning model.

Operations include

a) Cropping
b) Resizing
c) Pixel normalization
d) Face alignment
e) Noise reduction

Normalization can be represented as shown in equation 6

$$x' = (x - \mu) / \sigma$$

Equation 6

Where x is the original pixel value, μ is the mean and σ is the standard deviation. Facial landmarks like eyes, nose and mouth can be used to align the face.

d. *Anti-Spoofing*

Anti-spoofing classifies the presentation as Real or Spoof. The Model can use one or more visual properties:

a) Texture
b) Motion
c) Depth
d) Colour
e) Image quality
f) Frequency Characteristics
g) Temporal behavior

e. *Feature Extraction*

If the Presentation is classified as genuine, the system extracts a facial embedding.

f. *Identity Recognition*

The generated embedding is compared with registered embeddings in the database. Cosine similarity or Euclidean distance can be considered

8. AUTHENTICATION

The final decision is made by both stages. Let P = 1 denote a genuine presentation and P = 0 a spoof. Let R = 1 denote a successful identity match and R = 0 an identity mismatch. Authentication can be represented as shown in equation 7:

$$A = P \text{ AND } R$$

Equation 7

Thus, the system grants access only if the presentation is genuine and the identity matches a registered user.

9. DEEP LEARNING ANTI SPOOFING MODEL

a. *CNN Architecture*

A CNN can classify facial presentations. An example architecture includes:

Input Image → Convolution → Activation → Pooling → Convolution → Feature Representation → Fully Connected Layer → Real/Spoof Output

The convolution operation can be expressed as shown in equation 8:

$$Y(i, j) = \Sigma_m \Sigma_n X(i+m, j+n) K(m, n)$$

Equation 8

where X is the input image and K is the convolution kernel. Early layers can learn low-level features like edges and texture, while deeper layers can learn more complex visual patterns.

b. *Transfer Learning*

Training a deep network from scratch requires substantial data and computational resources. Transfer learning is an alternative, where a previously trained model on a large image dataset is adapted for the anti-spoofing task.The earlier layers can provide general

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

visual representations, and later layers are fine-tuned for genuine/spoof classification.

c. Texture Analysis

Texture differences are critical to print and replay attacks.

A printed photo can include:

i. Printing dots
ii. Paper texture
iii. Surface reflections
iv. Reduced skin detail

A display can include:

i. Pixel structures
ii. Moiré patterns
iii. Screen reflections
iv. Brightness differences

CNN models can learn these characteristics automatically.

d. Motion Analysis

A genuine person can naturally produce temporal changes. For a sequence F_1, F_2, F_3, …, F_n, the system can analyse changes between consecutive frames. Signals include blinking, head movement, eye movement, and facial expressions. Motion alone is insufficient, because a replayed video can contain realistic movement.

e. Depth Analysis

Depth information can provide additional discrimination. A genuine face contains three-dimensional structure, but a photograph is approximately two-dimensional. Depth can be obtained using stereo cameras, infrared cameras, time-of-flight sensors, or structured-light systems.

f. Temporal Information

Video-based anti-spoofing can analyze changes over time rather than a single frame. Temporal information can help identify differences between live facial movement and attack artifacts.

10. FACE RECOGNITION AND ANTI SPOOFING

After a presentation and been classified as genuine, the system proceeds to identify recognition. The facial recognition network generates an embedding from the detected face.

For example in equation 10:

$$E = [e_1, e_2, e_3, \ldots, e_n]$$

Equation 10

The input embedding is compared with registered templates, and a threshold is applied to the similarity score. If S ≥ T, the identity can be considered a , if S < T, the identity is rejected. The threshold should be experimentally chosen, as an overly low threshold can increase false acceptance, whereas an overly high false rejection. Thus, the two-stage authentication process becomes:

Stage 1: Presentation Attack Detection → Stage 2: Identity Verification → Authentication Decision

This arrangement ensures that an attacker cannot gain access simply by presenting an image resembling a registered user.

11. DATASETS AND TRAINING METHODOLOGY

A reliable dataset is necessary for developing an anti-spoofing model. Important datasets in face anti-spoofing research include:

- CASIA-FASD - provides genuine and spoofed sample and has been widely used for presentation attack detection.
- Replay-Attack - focues on replay and print presentation attacks under different conditions
- MSU-MFSD - the MSU Mobile Face Spoofing Databases has genuine and spoofed videos captured using different devices.
- OULU-NPU - designed to evaluate face anti-spoofing under multiple protocols and environmental variations.
- CelebA Spoofing - provides a large scale collection of facial images with expensive annotations and a broad range of spoofing characteristics.

Dataset Splitting

The dataset can be split into training, text and validation sets as shown in equation 9:

$$D = D_train \cup D_validation \cup D_test$$

Equation 9

The training set is used for learning model parameters, the validation set is for parameter selection and model tuning, and test set is for final evaluation. Leakage between subsets should be avoided - images of the same subject or highly similar sample should not unintentionally appear across training and test partitions.

Training Labels

For binary anti-spoofing classification: 0=Spoof, 1 = Genuine. The model learns a mapping from facial input to the probability of genuine presentation.

12. LOSS FUNCTION

Binary cross-entopy is appropriate for a binary classification task. The loss function is shown in Equation 10:

$$L = -[y \cdot \log(p) + (1 - y) \cdot \log(1 - p)]$$

Equation 11

Where y is the actual class label and p is the predicted probability. The model aims to minimizes the loss function during training, represented as shown in equation 11:

$$\theta^* = argmin_\theta\, L(\theta)$$

Equation 12

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

Where represents the trainable model parameters. Appropriate optimization methods, learning schedule, batch size, regularization, and early stopping can be experimentally chosen.

PERFORMANCE EVALUATION

Accuracy alone is not a sufficient metric to evaluate a biometric security system.

A. Accuracy

$$Accuracy = (TP + TN) / (TP + TN + FP + FN)$$

Equation 13

Represents the proportion of correctly classfied samples as shown in equation 12.

B. Precision

$$Precision = TP / (TP + FP)$$

Equation 14

Measures the proportion of predicted positive samples that are actually positive as shown in equation 13.

C. Recall

$$Recall = TP / (TP + FN)$$

Equation 15

Measures the proportion of actual positive samples that are correctly identified as shown in equation 14.

D. F1 Score

$$F1 = 2 \times (Precision \times Recall) / (Precision + Recall)$$

Equation 16

Provides a combined measure of precision and recall as shown in equation 15.

E. False Acceptance Rate

False Acceptance Rate measures the frequency with which unauthorized attempts are wrongly accepted:

FAR = False Acceptances / Total Impostor Attempts

A lower FAR is generally desired in an authentication system, although the appropriate operating point depends on ethe application.

F. False Rejection Rate

FRR = False Rejections / Total Genuine Attempts

Measures legitimate attempts that are incorrectly rejected.

G. Equal Error Rate

EER refers to the operating point where the false acceptance and rejection rates are approximately equal. These metrics should be considered together when evaluation a biometric authentication system.

13. EXPERIMENTAL SETUP

A prototype implementation can utilize a standard computer with a webcam and CPU processing. A possible software environment includes:

- Python
- OpenCV
- TensorFlow or PyTorch
- NumPy
- Scikit-learn
- Database software
- Web-based authentication interface

The implementation can follow this sequence:

1. Initialize camera.
2. Capture video frame.
3. Detect face.
4. Crop facial region.
5. Preprocess facial image.
6. Apply anti-spoofing model.
7. Reject if spoof is detected.
8. Generate facial embedding if genuine.
9. Compare embedding with registered templates.
10. Apply identity threshold.
11. Grant or reject access.
12. Record authentication event.

The system should be tested under a variety of environmental conditions, including changing lighting, camera position, facial pose, background, and attack presentation.

14. SECURITY AND PRIVACY CONSIDERATIONS

Facial biometric information requires careful security controls. A password can typically be changed after comprise, but facial characteristics cannot be replaced. Thus, storing facial information requires proper protection. Important security measures include:

A. Encryption

Biometric templates and communication channels should be protected using appropriate cryptographic mechanisms.

B. Access Control

Only authorized components and administrators should have access to biometric information.

C. Template Protection

Where practical, systems should avoid unnecessarily storing raw facial images. Protected templates or embeddings can be used, although embeddings should still be treated as sensitive biometric information.

D. Secure Communication

If Biometric information is transmitted between an application and server, secure communication protocols should be used.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

E. Data Retention

The system should define how long facial information is retained, and when it is deleted.

F. User Consent

Users should be informed about the purpose of biometric collection and how their information is processed.

G. Presentation Attack Resistance

H. The anti-spoofing module should be evaluated against multiple attack categories, rather than only one type of photograph.

15. APPLICATIONS

The combination of face recognition and anti-spoofing can be used in several application areas.

A. Attendance Systems

Anti-spoofing can prevent attempts to register attendance using photographs or videos of another person.

B. Access Control

The technology can facilitate contactless authentication for offices, laboratories, educational institutions, and controlled facilities.

C. Online Examination

Face anti-spoofing can determine whether the person appearing before the examination camera is physically present, rather than presented by a photograph or replayed video.

D. Banking

Facial authentication can integrated into selected financial applications as an identify-verification mechanism

E. Healthcare

Facial identification can assist with authorized access to certain digital systems while maintaining privacy safeguards.

16. EXPECTED OUTCOME

The proposed system will offer a unique outcome after analyzing the captured image or video through the camera. The following are the outcome of the designed system:

a. Face Detected: The output will be generated to indicate whether the face had been captured in the camera field or not.

b. Genuine Face: The output will be generated to acknowledge that the captured face is genuine; neither photo or any type of presentation attack (PA).

c. Spoof Detected: The output will be triggered if the system detects a presentation attack such as photo, video, screen, mask, and so on.

d. Face Recognition: The system will authenticate the captured face to recognize the user; therefore, the user should be registered in the database.

e. Authentication: The final step of the system will authenticate the captured face of an individual and provides access if the user is genuine or denied if the user is not genuine.

f. System Status: The unique output will indicate the final statues of the system after authentication is complete, and it is shown to the user.

For example, the following unique output shows the result after completing the detection process:

Face Detected: *YES*
Anti-Spoofing: *GENUINE*
User: *Registered User*
Authentication: *ACCESS GRANTED*

Another example shows the result of presentation attack:

Face Detected: *YES*
Anti-Spoofing: *SPOOF DETECTED*
Authentication: *ACCESS DENIED*

In general, the system first analyzes the camera field to detect a genuine face, and the second step is the face recognition to provide access to the legitimate users. Therefore, it is safe to say that the two-step procedure of the proposed system prevents presentation attacks efficiently.

17. ADVANTAGES AND LIMITATIONS

A. Advantages

The proposed system provides several architectural advantages:

1. Adds a presentation-attack detection stage prior to recognition.
2. Supports contactless authentication.
3. Can utilize ordinary RGB cameras for basic implementations.
4. Can incorporate video-based temporal information.
5. Can be extended using depth or infrared sensors.

B. Limitations

Dataset Dependency: A model trained on a limited collection of attacks may not perform equally well against unseen attack categories.

Illumination: Poor or changing lighting can affect both face detection and anti-spoofing.

Camera Dependency: Different cameras can produce different image characteristics, affecting model performance.

Computational Requirements: Deep neural networks may require substantial memory and processing resources.

Advanced Masks: Highly realistic three-dimensional masks may be challenging to distinguish from genuine faces using RGB information alone.

Synthetic Media: AI-generated and manipulated facial imagery can introduce additional challenges.

Privacy: Improper storage, sharing, or processing of facial biometric information can create security and privacy risks.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 11 , November - 2026

18. COMPARISON WITH FACE RECOGNITION-ONLY SYSTEMS

A conventional face recognition-only architecture primarily addresses the identity question. Its pipeline is:

Camera → Face Detection → Feature Extraction → Recognition → Authentication

The proposed architecture adds a security stage:

Camera → Face Detection → Preprocessing → Anti-Spoofing → Recognition → Authentication

The main difference is that the second architecture evaluates the authenticity of the facial presentation before matching identity.

19. CONCLUSION

Face recognition technology can be used for biometric verification purposes. However, it is vulnerable to photo, video, mask, and computer graphics spoofing. At the same time, the system described in the article will resolve this issue as it has an anti-spoofing modality, which allows distinguishing the real face from presentation attacks before identification.

The system described in the article can benefit from texture, motion, depth, and temporal information, apart from using deep learning algorithms. The efficacy of such a system can be evaluated using accuracy, precision, recall, F1-score, FAR, FRR, EER, and other metrics. The research described can be used in multimodal, vision transformers, edge AI, and privacy technologies to secure face authentication.

ACKNOWLEDGMENT

The authors thank the Department of Information Technology, PSG Polytechnic College, for the support provided during this project. We also thank our faculty guide, Mr. N. Ravi, for their guidance and support during the research.

REFERENCES

[1] IEEE, "A Review of Face Anti-Spoofing Methods for Face Recognition Systems," IEEE Xplore, Document 9548404.
[2] IEEE, "Deep Learning for Face Anti-Spoofing: A Survey," IEEE Transactions on Pattern Analysis and Machine Intelligence, Document 9925105, 2023.
[3] Springer, "Face anti-spoofing research," Multimedia Tools and Applications, Article s11042-019-08115-w.
[4] ScienceDirect, "An overview of face anti-spoofing methods for face recognition systems," Article S1047320326002476, 2026.
[5] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015.
[6] Z. Zhang et al., "A Face Antispoofing Database with Diverse Attacks," research associated with the CASIA Face Anti-Spoofing Database.
[7] I. Chingovska, A. Anjos, and S. Marcel, research on face presentation attack detection and replay attacks.
[8] A. George and S. Marcel, research associated with the OULU-NPU face anti-spoofing benchmark.
[9] Y. Zhang et al., "CelebA-Spoof: Large-Scale Face Anti-Spoofing Dataset with Rich Annotations," European Conference on Computer Vision (ECCV), 2020.
[10] Additional recent literature on deep learning, biometric authentication, presentation attack detection, domain generalization, multimodal anti-spoofing, and synthetic facial media should be incorporated according to the final experimental scope.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)