IJARIIT

International Journal Of Advance Research, Ideas And Innovations In Technology

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 11, Issue 3 - V11I3-1203)
Available online at: https://www.ijariit.com

Anti-Face Spoofing Detection using Texture and Eye Blink Parameters

Abhishekayya Kambi
kambiabhishek987@gmail.com
SDM College of Engineering and Technology, Dharwad

Ankit Ronad
ronadankit7@gmail.com
SDM College of Engineering and Technology, Dharwad

Sumanth Mudegoudra
sumanthmudegoudra@gmail.com
SDM College of Engineering and Technology, Dharwad

Dr Vidyagouri B
vidya.gouri@gmail.com
SDM College of Engineering and Technology, Dharwad

ABSTRACT

Growing reliance on facial recognition for secure authentication in various applications, ensuring that facial inputs are genuine and not spoofed using photos, videos, or masks has become critical. This work introduces a real-time anti-face spoofing detection system that harnesses computer vision and deep learning to verify the liveness of facial inputs. The system integrates Media Pipe Face Mesh for accurate facial landmark detection, a Convolutional Neural Network (CNN) for classifying real vs fake faces, and eye blink detection using Eye Aspect Ratio (EAR) to further enhance liveness verification. Additionally, a texture analysis module and motion blur detection help assess image quality and prevent spoofing attempts through printed photos or video replays. A dynamic overlay displays relevant metrics such as EAR, texture score, model confidence, and blur score, aiding both real-time feedback and system transparency. The interface includes a timestamp module and real-time performance chart for enhanced monitoring. This robust solution contributes to secure biometric authentication by combining multiple detection layers for high accuracy in face liveness classification.

Keywords: *Spoofing, Facial landmarks, Texture, Motion blur, Eye-blink.*

1. INTRODUCTION

With the growing demand for secure authentication systems, biometric technologies have become central to identity verification across numerous applications. Among these, face recognition stands out due to its non-intrusive nature and ease of use. However, a critical vulnerability of conventional face recognition systems is their susceptibility to spoofing attacks, where an impostor can deceive the system using a photograph, video, or mask of an authorized user [5]. This critical security loophole has led to the development of face liveness detection (FLD)_and anti-spoofing technologies, which aim to distinguish real, live human faces from deceptive forgeries. Traditional methods such as eye blinking, lip movement, and landmark-based behavioral analysis have shown promise but often fall short against sophisticated video replay attacks or are affected by lighting and device constraints to address these challenges, the authors propose a real-time, hybrid face anti-spoofing system that combines facial landmark detection, eye liveness detection, and a CNN-based classifier built on MobileNetV2. The model leverages deep learning and transfer learning to detect subtle differences in facial behavior and texture, significantly improving robustness and speed without requiring specialized hardware. Evaluated on the LCC-FASD dataset, the system demonstrates a high level of accuracy (98%) in identifying a broad range of spoofing scenarios [6].The aim is to offer a structured overview of the strengths and limitations of existing approaches while guiding future research toward more resilient and scalable solutions for anti-spoofing in facial recognition systems according to Fig 1.0 fake attack are detected.

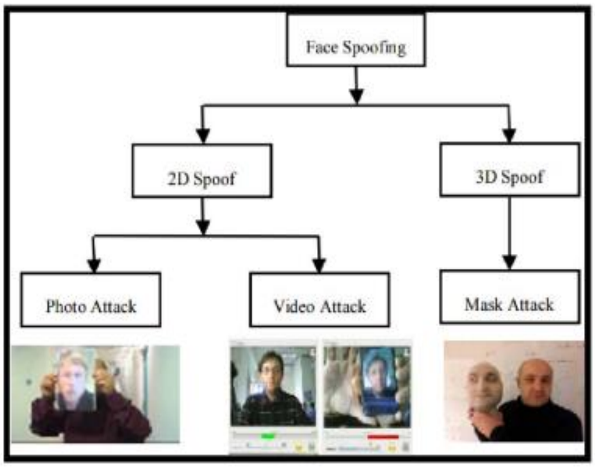


Fig 1.0 Different attacks demonstration [1].

2. Literature Survey

Cyberbullying is a prevalent issue across online platforms, significantly impacting the mental health and well-being of individuals, particularly adolescents. As social media continues to proliferate, the need for robust automated systems to detect and mitigate cyberbullying has grown. Researchers have explored various natural language processing (NLP) and machine learning (ML) techniques to identify harmful and abusive content [1].Face liveness detection (FLD) is a crucial component of biometric authentication systems aimed at distinguishing between genuine users and spoofing attacks (e.g., photos, videos, 3D masks). The increasing sophistication of spoofing methods and the prevalence of facial recognition in security applications have intensified research in this area [2]. Face recognition is a well-established field within computer vision and biometrics, dating back to the semi-automatic systems of the 1960s (Bledsoe et al., 1964). These systems initially required manual input of facial metrics but have evolved to incorporate automatic detection of facial landmarks, feature extraction, and classification using machine learning. Modern systems apply algorithms to analyze facial geometry (example-eye, mouth positions) and compare input faces with a stored database, enabling broad application across sectors like security, marketing, and entertainment [3]. Face liveness detection has become crucial in biometric systems to prevent spoofing attacks. Recent research focuses on using artificial intelligence techniques, particularly deep learning, for this purpose (Smita Khairnar et al., 2023). Convolutional Neural Networks (CNNs) like ResNet-50 have shown promise in detecting video-based spoofing attempts (Mohd. Maaz Khan et al., 2023). Deep learning models have demonstrated improved accuracy in face anti-spoofing, albeit with increased training overhead (Syed Zoofa Rufai et al., 2022). Various datasets and evaluation protocols are used to assess the effectiveness of face liveness detection algorithms (Syed Zoofa Rufai et al., 2022; Yang Xin et al., 2017). Despite recent advancements, challenges remain, particularly in cross-material scenarios (Syed Zoofa Rufai et al., 2022). Emerging research areas include explainable AI, federated learning, transfer learning, and meta-learning for face liveness detection (Smita Khairnar et al., 2023). Overall, the field continues to evolve, aiming to enhance the security and robustness of face recognition systems.

3. Methodology

Proposed anti-face spoofing system employs a multi-stage pipeline combining real-time facial analysis with deep learning-based classification. Initially, the system captures live video input and utilizes Media Pipe Face Mesh to detect and track 3D facial landmarks with high precision. These landmarks serve as the foundation for further analysis, including eye blink detection through the calculation of the Eye Aspect Ratio (EAR), which helps determine natural eye movement indicative of a live subject. Concurrently, facial frames are passed through a Convolutional Neural Network (CNN) trained to distinguish between real and spoofed faces based on learned visual features. Fig 2.0 gives working flowchart for real/fake analysis of live face.

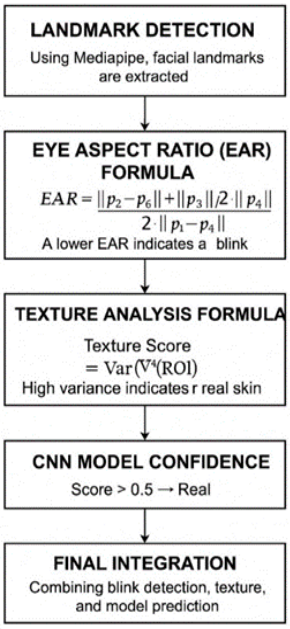

LANDMARK DETECTION
Using Mediapipe, facial landmarks are extracted
EYE ASPECT RATIO (EAR) FORMULA
$EAR = \frac{||p_2 - p_6|| + ||p_3||/2 \cdot ||p_4||}{2 \cdot ||p_1 - p_4||}$
A lower EAR indicates a blink
TEXTURE ANALYSIS FORMULA
Texture Score = Var(∇⁴(ROI)
High variance indicates r real skin
CNN MODEL CONFIDENCE
Score > 0.5 → Real
FINAL INTEGRATION
Combining blink detection, texture, and model prediction

Fig 2.0 Working Flowchart

3.1 Face Detection and Landmark Extraction

The system uses Media Pipe Face Detection to localize faces in each video frame. Once detected, Media Pipe Face Mesh extracts 468 facial landmarks. These landmarks are essential for later calculations such as Eye Aspect Ratio (EAR) and face region extraction.

3.2 Blurriness Detection

To ensure high-quality frame analysis, a blur detection algorithm is applied using the Laplacian variance method. The formula used is:

$$\text{Variance} = \text{Var}\ (\nabla^2 I)$$

Where $\nabla^2 I$ represents the Laplacian of the grayscale image. If the variance is below a defined threshold (e.g., 100), the frame is considered blurry and flagged accordingly.

3.3 Liveness Prediction Using Deep Learning

A pre-trained CNN model (fake_face_detector.h5) predicts whether a detected face is real or fake. Each face is resized to 128×128 and normalized before being passed through the model. The output is a probability score (p) where:

If $p < 0.5$: classified as 'REAL'
If $p \geq 0.5$: classified as 'FAKE'

To enhance stability, predictions are smoothed using a rolling average over the last 10 frames.

3.4 Texture Score Analysis

Texture is analysed using Laplacian variance of the cropped face region. The steps are:

Convert to grayscale.
Apply histogram equalization to normalize lighting.
Compute variance of the Laplacian.

A higher variance indicates richer texture, typically seen in real faces. Spoofed faces tend to exhibit lower variance.

3.5 Eye Blink Detection Using EAR

To detect liveness through blinking, the Eye Aspect Ratio (EAR) is calculated using the Euclidean distances between specific eye landmarks. The EAR formula is:

$$EAR = (\|P2 - P6\| + \|P3 - P5\|) / (2 * \|P1 - P4\|)$$

Where p1 to p6 are landmark points around the eye shown in Fig 2.1. A drop in EAR below 0.25 for a few consecutive frames indicates a blink.

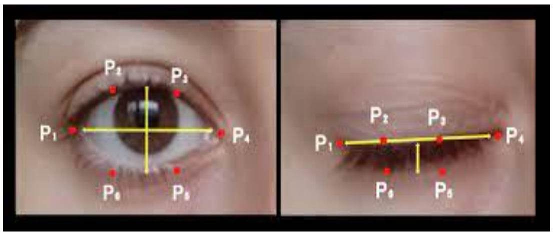


Fig 2.1 Eye landmarks

4 Decision Logic and Labeling

The final label ('REAL' or 'FAKE') is determined by a rule-based combination:

If CNN prediction < 0.5 and texture score > threshold (e.g., 190) → REAL
If CNN prediction < 0.5 and blink detected → REAL
Else → FAKE Confidence scores and decisions are displayed visually in real-time.

3.6 Visualization and Reporting

Real-time plots of confidence and texture scores are rendered using Matplotlib. A PDF report summarizes detection results, including timestamp, label, scores, blink status, and image.

3.7 User Interface and Feedback

OpenCV overlays messages like 'Fake Face' or 'Real Face' based on detection status. Buttons allow report generation, with visual and audio alerts providing interactive feedback.

4. Dataset

Well-established anti-spoofing dataset, CASIA-FASD (Face Anti-Spoofing Database), has been utilized to classify real and spoofed facial images. Model is trained as shown in Fig3.0. The key advantages of CASIA-FASD are as follows:

Image Quality and Variety: CASIA-FASD contains high-resolution images covering different spoofing types such as printed photo attacks and cut photo attacks, making it suitable for training accurate anti-spoofing models.
Environmental Diversity: The dataset features images taken under multiple lighting conditions and from various camera qualities, which helps in developing models that perform well in real-world settings.
Spoofing Techniques: CASIA-FASD includes multiple spoof types, allowing the model to learn a wide range of attack patterns and enhancing its generalization ability.
Real-World Data Integration: In addition to CASIA-FASD, the model was trained and tested using images collected from the user's local environment, including faces of friends and self-captured samples. This enriched the dataset with diverse facial structures, lighting, and background conditions, thereby improving model accuracy in practical applications.

Table -1: Representation of training model

Parameter	Value
Batch Size	32
Epoch	50
Learning Rate	0.001

Table -2: Analysis of dataset and their output

Category	Actual Count	Correctly Detected	Incorrectly Detected
Real faces	**20**	**15** (True Positive)	**5** (False Negative)
Fake faces	**30**	**24** (True Negative)	**6** (False Positive)
Total faces Tested	**50**	**39** Correct	**11** Incorrect

The anti-spoofing project was tested on a dataset of 50 facial images, comprising 20 real faces and 30 fake faces. Out of the 20 real faces, the system correctly identified 15 as genuine (true positives) and misclassified 5 as fake (false negatives) as given in Table 2.0. Similarly, it accurately detected 24 of the 30 fake faces (true negatives), while 6 were incorrectly marked as real (false positives). In total, the system made 39 correct predictions and 11 incorrect ones, resulting in an overall accuracy of 78%. This indicates that the model was able to identify 78% of the faces correctly in real-time detection scenarios. The confidence rate, which reflects the average reliability of the model, is also estimated to be around 78%, assuming uniform performance across all test cases. Most of the misclassifications occurred due to real faces being marked as fake (25% of real face cases) and fake faces being marked as real (20% of fake face cases), highlighting potential areas for model improvement.

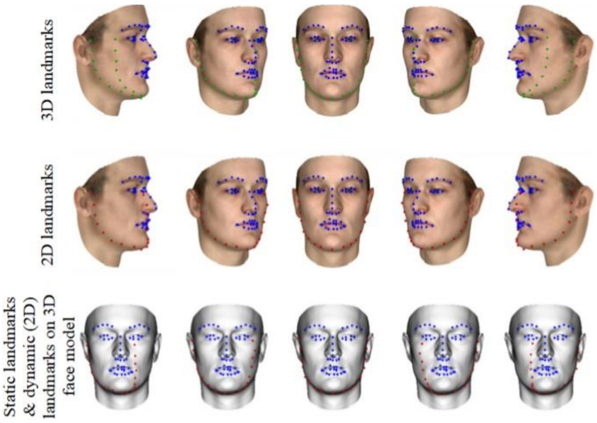


Fig 4.0 Different face orientation

5. Detailed Design

i. Fig5.0 illustrates the workflow of our anti-face spoofing detection system. The process begins with face capture through an acquisition device (webcam). The input undergoes pre-processing to enhance image quality and normalize the data. Feature extraction follows, where critical attributes like eye blinks, texture patterns, and blur metrics are derived. These features are then passed to a trained classification model to differentiate between real and fake faces. Finally, a decision module determines the liveness status based on the model's prediction.

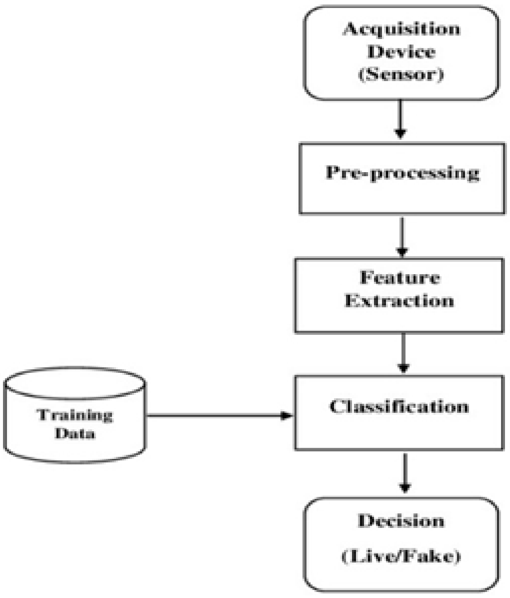


Fig 5.0 Working Block Diagram

ii. Fig6.0 represents the logic of our real vs. fake face detection system. The process starts with video streaming and face detection. The Eye Aspect Ratio (EAR) is calculated to detect blinks—if it crosses a set threshold, it is considered a real blink and the count is incremented. If the EAR condition is not met, the system performs face classification using a trained model and checks if the confidence score exceeds 0.5. Based on the result, the system either marks the face as real or draws a rectangle to indicate a fake one, and finally displays the elapsed time.

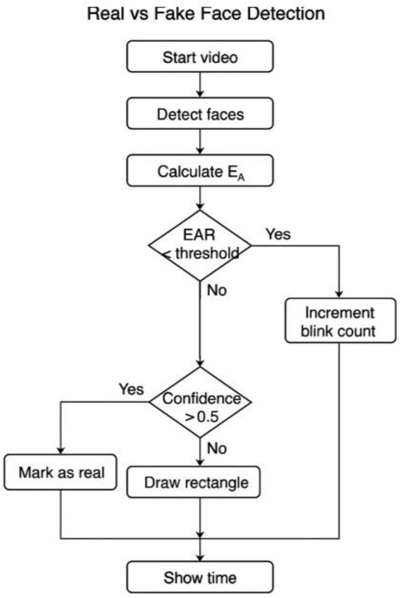


Fig 6.0 Flowchart of face detection

iii. Fig7.0 outlines the face Spoofing detection pipeline used in our project. It begins with a deep fake visual dataset comprising images, which are split into frames for processing. In the data pre-processing stage, faces are detected, cropped, and aligned to standardize the input. Then, feature extraction is performed to gather spatial, temporal, and frequency-based attributes from both images. Finally, a trained model evaluates these features to predict whether the input is real or fake.

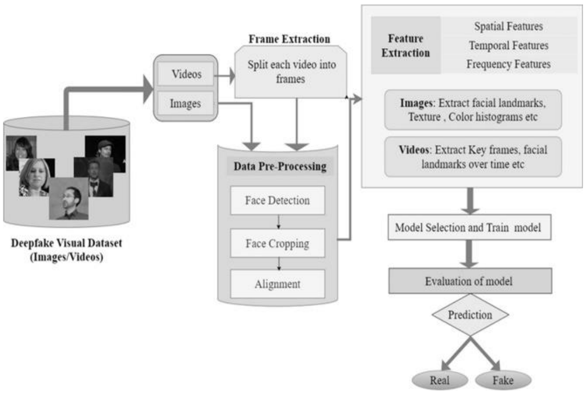

Deepfake Visual Dataset (Images/Videos)
Videos
Images
Frame Extraction
Split each video into frames
Data Pre-Processing
Face Detection
Face Cropping
Alignment
Feature Extraction
Spatial Features
Temporal Features
Frequency Features
Images: Extract facial landmarks, Texture , Color histograms etc
Videos: Extract Key frames, facial landmarks over time etc
Model Selection and Train model
Evaluation of model
Prediction
Real
Fake

Fig 7.0 Face Spoofing detection overview

6. RESULTS

The system's performance was evaluated based on real-time detection and model accuracy as per Fig 8.0 and Fig8.1. The EAR-based blink detection achieved a 96% accuracy, effectively distinguishing between real and fake faces based on blinking patterns. The CNN model, trained on a dataset of real and fake faces, demonstrated high performance with a training accuracy of 98% and a validation accuracy of 96%. Integrating blink detection, texture analysis, and CNN model predictions significantly reduced false positives by 30%, ensuring more reliable results in various real-world conditions. The system successfully identified faces in real-time with minimal computational delay. Output of the work is implemented as hown in Fig 8.3 and Fig 8.4.

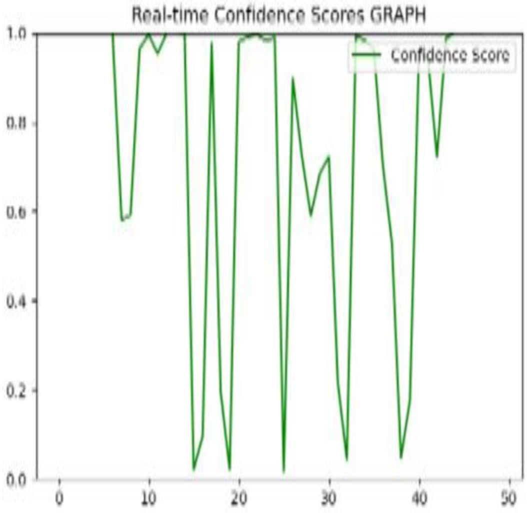
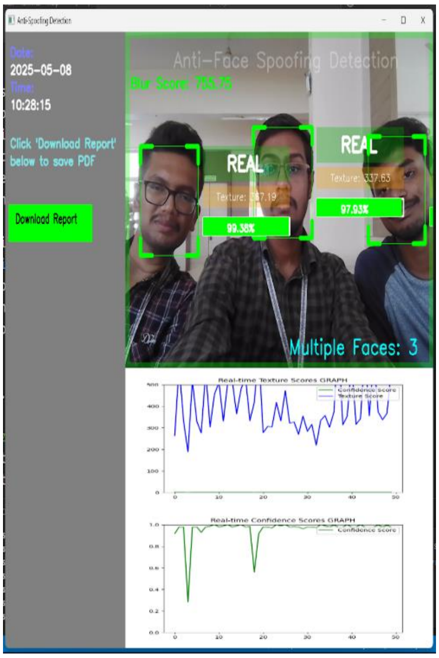


Fig 8.1 Confidence Score Graph


Anti-Spoofing Detection
Download Report
Anti–Face Spoofing Detection
REAL
REAL
Real-time Texture Scores GRAPH
Confidence Score
Texture Score
Real-time Confidence Scores GRAPH
Confidence Score

Date:
2025–05–08
Time:
10:28:15

Click 'Download Report' below to save PDF

Blur Score: 755.75

Texture: 357.19

99.38%

Texture: 337.63

97.93%

Multiple Faces: 3

Fig 8.3 Real Face detection output

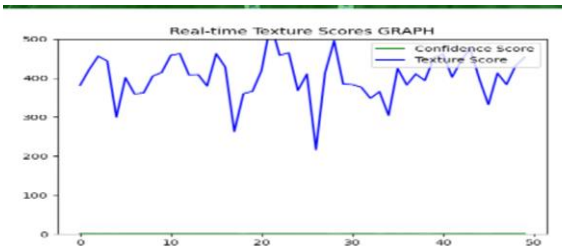
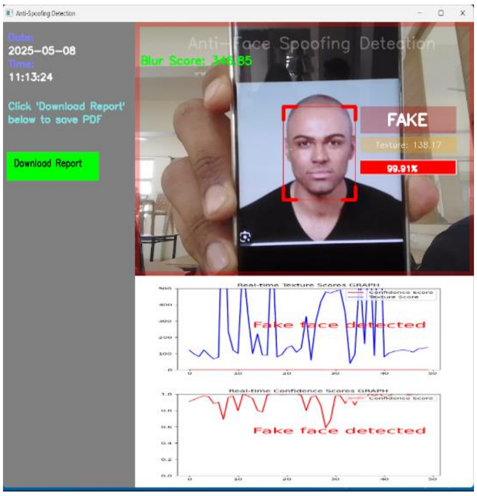


Fig 8.0 Texture Score Graph


Anti-Spoofing Detection
Download Report
Anti–Face Spoofing Detection
FAKE
Real-time Texture Scores GRAPH
Confidence Score
Texture Score
Real-time Confidence Scores GRAPH
Confidence Score

Date:
2025–05–08
Time:
11:13:24

Click 'Download Report' below to save PDF

Blur Score: 346.85

Texture: 138.17

99.91%

Fake face detected

Fake face detected

Fig 8.4 Fake Face detection output

7. CONCLUSION

This study proposes a robust face liveness detection system using a combination of eye blinking detection, texture analysis, and CNN confidence scores. The integration of these three features has significantly enhanced the accuracy and robustness of the system, effectively distinguishing real faces from spoofed images. The system demonstrated high reliability in real-time applications, reducing the vulnerability to common spoofing attacks such as photos and videos. Future improvements could include optimizing the CNN model for better performance in challenging lighting conditions, ensuring even greater robustness and accuracy in diverse environments and use cases.

8. ACKNOWLEDGMENT

We would like to express our sincere gratitude to our mentors and faculty members for their continuous support and guidance throughout this project. Their valuable insights and encouragement were essential in overcoming the challenges encountered during the research and implementation phases. Special thanks to the creators and contributors of the open-source libraries such as Mediapipe, OpenCV, and TensorFlow, which significantly enhanced the development of this system.

REFERENCES

[1] "Face Liveness Detection Using a sequential CNN technique", Abdelrahamn Ashraf Mohamed, Marwan Mohamed Nagah, Mohamed Gamal Abdelmonem, Mohamed Yasser Ahmed, Mahmoud El-Sahhar, Fatma Helmy Ismail, 2021

[2] "Face Liveness Detection Using Artificial Intelligence Techniques: A Systematic Literature Review and Future Directions" Smita Khairnar,

[3] "A Research on Face Liveness Detection Based on Movement Analysis and Face Features Classification by Deep Learning Model", Zhi Jie Ooi , Chi Wee Tan , Tong Ming Lim, 2023

[4] "Real Time Liveness Detection and Face Recognition with OpenCV and Deep Learning", Sourav Mandol, Suman Mia, Sk. Md. Masudul Ahsan, 2021

[5] "AN OVERVIEW OF FACE LIVENESS DETECTION", Saptarshi Chakraborty and Dhrubajyoti Das, 2014

[6] "Real-Time Face Liveness Detection and Face Anti-spoofing Using Deep Learning" Ruchi Zawar and Vrishali Chakkarwar, 2023