International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Liveness Detector for Face Recognition System Fake Vs Real

RAMYA N[1],SANDHIYA T[2],SONI S[3],PRIYADHARSHINI S[4],SUMITHRA V[5]

[1]Assistant Professor -Department of Information Technology & Kings Engineering College-India.

[2,3,4,5]Department of Information Technology & Kings Engineering College-India.

Abstract - facial recognition systems are increasingly deployed for identity verification and security, but they remain vulnerable to spoofing attacks using photographs, videos, or 3D masks. To address these challenges, a liveness detection mechanism is critical to distinguish between real, live human faces and spoofed or fake inputs. This paper presents a liveness detection framework integrated with a facial recognition system, utilizing techniques such as eye-blink detection, facial micro- movements, texture analysis, and 3D depth estimation. The proposed system aims to enhance the security of face-based authentication by rejecting spoofed attempts in real-time, with minimal latency and high accuracy. Experimental results demonstrate the effectiveness of the approach across a variety of spoofing scenarios, including printed photos and digital screen replays. Face recognition is a widely used biometric approach. Face recognition technology has developed rapidly in recent years and it is more direct, user friendly and convenient compared to other methods. But face recognition systems are vulnerable to spoof attacks made by non-real faces. It is an easy way to spoof face recognition systems by facial pictures such as portrait photographs. And face forthe development of technology recently, almost all universities in Indonesia have implemented online attendance. An online attendance system using facial recognition is a technology that is able to identify a person's face from a digital image

***Key Words*:** eye-blink detection, 3D , face forthe , digital image, facial recognition, convenient

1. INTRODUCTION

Biometric authentication, particularly facial recognition, has gained widespread adoption in modern security systems due to its convenience and contactless nature. However, these systems are susceptible to spoofing attacks where an attacker uses a photo, video, or even a 3D mask of an authorized user to gain unauthorized access. This vulnerability poses significant security risks, especially in sensitive applications such as mobile banking, access control, and national identification systems.

Liveness detection, also known as presentation attack detection (PAD), is an essential enhancement to facial recognition systems that helps determine whether the presented face belongs to a live human being or is a spoofed artifact. Traditional facial recognition systems without liveness detection can be easily fooled by high-quality printed images or digital video replays.

Therefore, integrating robust liveness detection mechanisms can significantly strengthen the resilience of these systems.

This work aims to contribute a reliable, efficient, and easy-to-integrate liveness detection module that can be deployed alongside existing facial recognition systems to enhance overall biometric security. growing segment of such security industry.

Some of the familiar techniques for identification are facial recognition, fingerprint recognition, handwriting verification, hand geometry, retinal and iris scanner. Among these techniques, the one which has developed rapidly in recent years is face recognition technology and it is more direct, user friendly and convenient compared to other methods.

Therefore, it has been applied to various security systems. But, in general, face recognition algorithms are not able to differentiate ‘live’ face from ‘not live’ face which is a major security issue.

It is an easy way to spoof face recognition systems by facial pictures such as portrait photographs. In order to guard against such spoofing, a secure system needs liveness detection. The general public has immense need for security measures against spoof attack. Biometrics is the fastest growing segment of such security industry. Some of the familiar techniques for identification are facial recognition, fingerprint recognition, handwriting verification, hand geometry, retinal and iris scanner.

This work aims to deliver a reliable, efficient, and easily integrable liveness detection module to strengthen existing facial recognition systems and prevent spoofing attacks. While face recognition has become one of the fastest-growing and user-friendly biometric methods—more convenient than fingerprints or iris scans—it struggles to distinguish between live faces and static images.

This vulnerability allows attackers to bypass systems using photographs or masks. Therefore, integrating liveness detection is critical for enhancing biometric security. With increasing demand for robust identity verification, especially in the face of spoofing threats, liveness detection plays a key role in securing modern facial recognition technologies.

2. FACE RECOGNITION SYSTEM OVERVIEW

2.1 Basics of Face Recognition

Face recognition involves detecting, aligning, and extracting features from facial images to match them against a database. Techniques include 2D/3D recognition, geometric and deep learning-based features (like CNNs). It supports both **verification** (1:1) and **identification** (1:N).

2.2 Applications
Used in security (airports, law enforcement), device authentication, retail analytics, healthcare (patient ID), and online education (exam proctoring).

2.3 Challenges
Accuracy is affected by pose, lighting, facial expressions, occlusions (like masks), aging, and demographic bias. Spoofing remains a major threat—hence, the need for robust liveness detection.

2.4 System Requirements
Hardware: Core i5 processor, 4GB RAM, monitor, keyboard, and mouse.
Software: Python (via PyCharm IDE).

Python is a versatile, high-level programming language known for its clear syntax, portability, and extensive libraries. PyCharm, a cross-platform IDE by JetBrains, enhances productivity. Python's evolution was influenced by languages like ABC and Modula-3, designed to support extensibility and robust error handling—key for building reliable systems like this one.

3. PRESENTATION ATTACKS AND SPOOFING

3.1 Types of Spoofing Attacks

Spoof Type	Common Tools Used
Photo Attack	Printed photo or image on a mobile
Video Replay	Phone or tablet displaying a video
3D Mask Attack	Silicone or resin face masks
Digital Injection	Software-based image injection

3.2 Impact on Security

Impact Area	Description
Authentication	Unauthorized access to apps or devices
Data Breach	Leakage of personal and sensitive information
Financial Loss	Fraudulent transactions or identity misuse
System Trust	Reduced confidence in biometric systems
Legal & Privacy	Legal implications due to weak security measures

3.3 Data Acquisition
Real and spoofed face images are collected for both training and testing purposes. Images are captured at a distance and adjusted for clarity before inclusion in the dataset.

3.4 Data Collection & Preprocessing

- **Dataset Used:** RealDF-FakeFace, a merged dataset of real and fake faces.
- **Distribution:** Includes 299 real / 712 fake for training and 340 real / 178 fake for testing.
- **Preprocessing:** Images undergo resizing, normalization, and noise reduction.
- **Face Detection:** YOLO or deep learning detectors locate face regions.
- **Feature Extraction:** Techniques include texture analysis, color histograms, or deep features (e.g., VGG).
- **Liveness Detection:** Software techniques assess whether the input is from a live person or a spoof. A confidence score helps classify the face as real or fake.

4. LIVELINESS DETECTION TECHNIQUES

4.1 Definition and Importance
Liveness detection determines whether a biometric input (e.g., a face) comes from a live person rather than a spoofed source like a photo, video, or mask.
Significance:

- Prevents spoofing and identity fraud
- Enhances biometric authentication security
- Builds trust in facial recognition systems

4.2 Hardware-Based Approaches
Utilizes specialized devices to detect physiological cues of a live person.

Hardware	Function
3D Depth Camera	Captures facial depth and structure
Infrared (IR) Sensor	Detects live skin reflectivity and warmth
Thermal Camera	Measures body heat emitted by a real face
Ultrasound/Time Sensors	Evaluates facial geometry using acoustic signals

Pros: High accuracy, strong resistance to spoofing
Cons: Costly, may not be suitable for all devices

4.3 Software-Based Approaches
Software-only methods use visual data and algorithms to detect liveness:

- **Texture Analysis:** Detects anomalies in skin texture using LBP, Gabor filters, CNNs

- **Motion Analysis:** Tracks subtle facial movements and natural motion
- **Eye Blink Detection:** Monitors frequency and realism of blinking
- **3D Face Estimation:** Differentiates flat photos from real 3D faces
- **Challenge-Response:** Prompts actions like blinking or head movement

Pros: Affordable and adaptable to consumer devices
Cons: Less robust under poor lighting or replay attacks

4.4 Hybrid Approaches

Combines both hardware and software for enhanced security.

Examples:

- IR camera + blink detection
- Depth sensing + texture and motion analysis

Advantages:

- Greater accuracy and robustness
- Fewer false positives and negatives

Drawbacks:

- Increased cost and system complexity

5. DATASET AND BENCHMARKING

5.1 Public Datasets

Public datasets play a key role in training and evaluating face recognition and detection models. They provide:

- Large, annotated image sets.
- Variations in pose, lighting, age, expression, and occlusion.
- A standardized basis for comparing different models.

Key datasets include:

- **LFW**: 13,000 images for face verification.
- **CASIA-WebFace**: 494,000 images for model training.
- **VGGFace2**: 3.3 million images for large-scale training.
- **MS-Celeb-1M**: 10 million images for deep recognition tasks.
- **CelebA**: 200,000 images used for face verification and attribute classification.
- **WIDER FACE**: 32,000 images for face detection in complex environments.
- **FDDB**: 2,800 images used to evaluate face detection under occlusion.

These datasets support a range of applications such as face verification, recognition, and benchmarking in real-world conditions.

5.2 Evaluation Metrics

Performance metrics for face recognition systems help evaluate and compare models:

- **Precision & Recall**: Measures the accuracy and completeness of detected faces.
- **Mean Average Precision (mAP)**: Used to assess detection performance.
- **Accuracy**: Proportion of correct predictions.
- **True Positive Rate (TPR) / False Positive Rate (FPR)**: Measures how well a system correctly identifies or misidentifies faces.
- **Receiver Operating Characteristic (ROC) Curve**: Evaluates performance by plotting TPR vs. FPR.
- **Equal Error Rate (EER)**: The point where false acceptance and false rejection rates are equal.

5.3 Benchmark Results

Common benchmarking challenges include:

- **NIST FRVT**: Standardized testing for face recognition systems.
- **MegaFace Challenge**: Evaluates recognition at scale (1 million distractors).
- **IJB Series**: Used for testing face verification and clustering under challenging, unconstrained conditions.

5.4 Comparison of Real vs Fake Detection

As spoofing technologies, like deepfakes, advance, detecting real vs fake faces becomes increasingly difficult. Effective detection systems use metrics such as accuracy, precision, recall, and F1-score to evaluate performance.

Key methods for detecting fake faces include:

- **Deep Learning (CNN, RNN, Transformers)**: High performance and adaptability to various spoofing types, but requires large datasets and may overfit if not managed carefully.
- **Handcrafted Features**: Effective for detecting known spoof patterns like lighting inconsistencies but less capable of generalizing to new or subtle attacks.

Key performance metrics like **ROC**, **AUC**, and **EER** help assess the robustness of these systems against spoofing attacks.

6. MACHINE LEARNING DETECTION

6.1 YOLOv8

YOLOv8 is the latest state-of-the-art model in the YOLO series for object detection, image classification, and instance segmentation tasks. Developed by Ultralytics, which also created YOLOv5, YOLOv8 introduces several architectural changes and developer experience improvements. It continues to be under active development as Ultralytics responds to community feedback and works on new features.

The YOLO (You Only Look Once) series has become well-known for its accuracy, small model size, and accessibility. YOLO models can be trained on a single GPU, making them suitable for low-cost deployments on edge hardware or in the cloud. Initially launched in 2015 by Joseph Redmond, YOLO has evolved significantly, with YOLOv5 becoming the standard in the field, supporting a vibrant community that actively contributes improvements and new techniques.

6.2 YOLO ARCHITECTURE

While YOLOv8 does not have a published research paper yet, its architecture and improvements are based on the work done in the YOLOv5 repository. YOLOv8 builds upon the strong fundamentals of YOLOv5, incorporating community-driven improvements to enhance accuracy and efficiency.

6.3 FEATURE EXTRACTION METHODS

In machine learning-based detection, handcrafted features are used to differentiate real and spoofed inputs:

- **Texture-based Features**: Local Binary Patterns (LBP), Histogram of Oriented Gradients (HOG), Gabor filters.
- **Frequency-based Features**: Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) to analyze spoof-specific frequency patterns.
- **Motion and Depth Cues**: Optical flow for detecting eye blinking or lip movement; disparity maps for identifying 3D structures.

Other hand-crafted features include color space analysis (YCbCr, HSV) to detect color inconsistencies in spoof media.

6.4 RECENT ADVANCES

- **A. Transformer-based Models**: Vision Transformers (ViT) and Swin Transformers are now used for spatial feature extraction and have shown strong performance in passive spoof detection.
- **B. 3D Face Reconstruction**: These models reconstruct 3D faces from 2D inputs to detect flat fakes, using depth maps or point clouds (e.g., PRNet).
- **C. Multi-modal Approaches**: Combining RGB with infrared (IR), depth sensors (e.g., Intel RealSense), or thermal imaging to enhance spoof detection.
- **D. Anti-Spoofing Benchmarks**: Public datasets such as CASIA-FASD, Replay-Attack, OULU-NPUSiW, and SiW-M are used for evaluating anti-spoofing performance.

7.CONCLUSION

This work provided an overview of different approaches of face liveness detection. It presented a categorization based on the type of techniques used and types of liveness indicator/clue used for face liveness detection which helps understanding different spoof attacks scenarios and their relation to the developed solutions. A review of most interesting approaches for liveness detection was presented. The most common problems that have been observed in case of many liveness detection techniques are the effects of illumination change, effects of amplified noise on images which damages the texture information. Furthermore, the datasets, which play an important role in the performance of liveness detection solutions, must be informative and diverse that mimics the expected application scenarios. Non- interactive video sequences must include interactive sequences where the users perform certain tasks. Future attack datasets must consider attacks like 3D sculpture faces and improved texture information. Our main aim is to give a clear pathway for future development of more secured, user friendly and efficient approaches for face liveness detection.

ACKNOWLEDGEMENT

We thank **God Almighty** for the blessings, knowledge and strength in enabling us to finish our project. Our deep gratitude goes to our founder **Late. Dr. D. SELVARAJ, M.A., M.Phil.,** for his patronage in completion of our project. We take this opportunity to thank our kind and honourable **Chairperson, Dr. S. NALINI SELVARAJ, M.Com., M.Phil., Ph.D.,** and our **Honourable Director, Mr. S. AMIRTHARAJ, B.Tech., M.B.A** for their support to finish our project successfully. We wish to express our sincere thanks to our beloved **Principal, Dr.C.RAMESH BABU DURAI M.E., Ph.D.,** for his kind encouragement and his interest toward us. We are grateful to **Dr.D.C.JULLIE JOSPHINE M.E., Ph.D., Professor and Head of INFORMATION TECHNOLOGY DEPARTMENT,** Kings Engineering College, for his valuable suggestions, guidance and encouragement. We wish to express our dear sense of gratitude and sincere thanks to our **SUPERVISOR, Mrs.RAMYA N M.E.,** Assistant Professor, Information Technology Department. for her internal guidance. We

express our sincere thanks to our parents, friends and staff members who have helped and encouraged us during the entire course of completing this project work successfully

REFERENCES

1. R. Shao, X. Lan, P.C. Yuen, Joint discriminative learning of deep dynamic textures for 3D mask face anti-spoofing, IEEE Trans. Inf. ForensicsSecur. (2018).

2. J. Liu, A. Kumar, Detecting presentation attacks from 3D face masks under multispectral imaging, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2018, pp. 47–52.

3. S. Liu, P.C. Yuen, S. Zhang, G. Zhao, 3D mask face anti-spoofing with remote photoplethysmography, in: European Conference on Computer Vision, Springer, 2016, pp. 85–100.

4. X. Li, J. Komulainen, G. Zhao, P.C. Yuen, M. PietikÃn, Generalized face anti-spoofing by detecting pulse from face videos, in: International Conference on Pattern Recognition, 2017, pp. 4244– 4249.

5. S.-Q. Liu, X. Lan, P.C. Yuen, Remote photoplethysmography correspondence feature for 3d mask face presentation attack detection, 2018, pp. 558–573.

6. J. Hernandez-Ortega, J. Fierrez, A. Morales, P. Tome, Time analysis of pulse-based face anti-spoofing in visible and NIR, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2018, pp. 544–552.

7. A. Ali, N. Alsufyani, S. Hoque, F. Deravi, Biometric counter-spoofing for mobile devices using gaze information, in: International Conference on Pattern Recognition and Machine Intelligence, Springer, 2017, pp. 11–18.