IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A SURVEY ON FACE ANTI-SPOOFING AI TOOLS IN MODERN AUTHENTICATION SYSTEMS

Satish Kumar Nath
Lecturer (Computer Engineering)
Board of Technical Education, Rajasthan, Jodhpur

ABSTRACT

As biometric systems increasingly become embedded in the financial, governmental, and personal security systems, the accuracy of face recognition technology has become critical. At the same time, there is a growing number of Presentation Attacks (PA) and synthetic media, which are not covered by legacy static detection. This research paper provides an in-depth review of the current face anti-spoofing (FAS) tools employed in current authentication systems in 2026. We look at enterprise-grade solutions and open-source frameworks, and discuss them based on technical methods: from the traditional texture-based approach to cognitive, multimodal, and edge-based liveness detection. Moreover, the compliance with international security standards [1] is analyzed. This survey offers a structured overview of the effectiveness of these tools in mitigating threats like high fidelity 3D masks, digital replay attacks and deepfake manipulations using AI.

Keywords: Face Anti-Spoofing, Synthetic Media Detection, Multimodal Biometrics, Deepfake Analysis

I. INTRODUCTION

Biometric authentication has evolved into the cornerstone of identity verification in the digital ecosystem. This facilitates a secure access to banking, government services, and public infrastructure. With the success of basic facial recognition algorithms [2] in matching authorized users with high accuracy, the new security constraint is now on the input layer. Along with the paradigm shift towards the convenience of password-less authentication, there has been an increase in attacks called Presentation Attacks (PA) that take advantage of the optical vulnerabilities that exist in digital sensors [3].

The most important problem in the modern authentication is the "Liveness" problem. The synthesis of human likeness has become a commodity with the proliferation of readily available Generative Adversarial Network (GAN) tools, and high fidelity deepfakes. The capacity to generate human likeness has been commoditized with the proliferation of readily available Generative Adversarial Network (GAN) tools and high fidelity deepfakes [4]. More and more, high-quality liveness tests based on the motion of the face or head are now being replaced by sophisticated AI models that can reproduce these motions with high fidelity [5]. This research paper systematically reviews the current status of the face anti-spoofing technology and compares commercial products and powerful open-source frameworks to offer a path towards secure, user-centric biometric pipelines [6].

II. TAXONOMY AND MECHANISMS OF PRESENTATION ATTACKS

Biometric spoofing has evolved into a specialized, tiered classification of attack vectors. Modern academic and enterprise tools need to counteract:

1. Physical Presentation Attacks: These use the physical constraint of the typical RGB mobile sensors [7]. They are commonly conducted via high-resolution print attacks, digital screen replay attacks and high fidelity 3D silicone or latex masks [8]. The attacks are based on sensor's inability to distinguish between the human epidermis and material reflections.

2. Digital Injection and Synthetic Attacks: The threat environment has evolved to include digital manipulation (digital injection and synthetic attacks). Deepfakes and GAN-generated faces are fed directly into the Verification pipeline, and sometimes into a virtual camera application or through a malicious API interception [9]. The attacks are mathematical mimicry attacks, which are usually not detected by the traditional sensor-level hardware-based checking [10].

III. METHODOLOGY AND EVALUATION METRICS

The identified AI tools are evaluated using industry standard metrics, as outlined in ISO/IEC 30107-3 [1]:

1. Attack Presentation Classification Error Rate (APCER): Percentage of attacks incorrectly identified as valid (legitimate) users. The smaller the APCER, the more resistant the system is to unauthorized access [11].

2. Bona Fide Presentation Classification Error Rate (BPCER): Percentage of legitimate users incorrectly identified as spoof attacks. If the BPCER is high, users may become frustrated and abandon the system [11].

3. Half Total Error Rate (HTER): The average of APCER and BPCER (arithmetic mean); HTER is used as a key indicator to measure the balance between security and usability of the system in complex datasets [11].

IV. SURVEY OF AI-BASED ANTI-SPOOFING TOOLS

The Face Anti-Spoofing (FAS) tools available in year 2026 show a distinct division between high-availability commercial enterprise platforms and research-driven open-source frameworks.

A. ACADEMIC AND ENTERPRISE SOLUTIONS

1. Amazon Rekognition Face Liveness: Amazon Rekognition is built on a cloud-native, multi-frame temporal video analysis architecture to support physical presentation attacks and digital media manipulation detection. The system is designed to process short video streams for the purpose of tracking the photometric consistency of the face over time, and to detect inconsistencies in frame rates, colour changes and moiré patterns (the characteristic high-frequency noise pattern produced when a digital screen is rephotographed) [12].

2. SpoofSense: SpoofSense overcomes the latency limitations of mobile-first authentication, introducing the world's first single-frame micro texture analysis. The tool can assess the target's light scatter across the target, making it possible to distinguish the light scatter of human skin from synthetic materials like engineered latex, printed paper, or silicone resins [13].

3. Oz Liveness: Designed to withstand 3D mask attacks and advanced video injection in highly controlled environments, Oz Liveness is engineered to provide resistance. The platform assesses the consistency of depth and the reflections of the light in the environment. It monitors the light falling on the geometry of the face, and instantly identifies the "unnatural" and "uniform" reflectivity characteristic of artificial surfaces.

4. InsightFace (InspireFace SDK): InsightFace has an edge-native framework for real-time local processing. It uses highly optimized, quantized neural networks with additive angular margin losses to achieve local extraction of deep facial landmarks and liveness vectors within IoT access gates and mobile chipsets [14]. This by itself meets tight privacy standards such as GDPR, which have a focus on protecting data in transit.

B. OPEN-SOURCE FRAMEWORKS AND ACADEMIC BASELINES

1. Silent-Face-Anti-Spoofing (MiniVision): A lightweight, open-source repository for resource-constrained edge systems, Silent-Face-Anti-Spoofing. The framework uses a simplified Convolutional Neural Network (CNN) that is supervised by auxiliary depth supervision and structural pruning [15]. It is designed to be the main defensive tool against 2D print and screen replay attacks against low-power embedded devices, such as ATVs, tractors, and other agricultural machinery.

2. DeepFace: DeepFace is a python framework around popular deep learning facial recognition models [14] that is flexible enough to be used in a variety of applications. It offers researchers a modular pipeline for extracting deep representation vectors and passing them to custom Presentation Attack Detection classifiers, while maintaining the overall recognition accuracy.

3. Swin Transformer V2: This architecture is the state-of-the-art academic baseline that moves away from the conventional CNN to hierarchical vision transformer (ViTs) [6]. It is able to detect long-range structural dependencies and micro-level patch anomalies. It has been trained on a variety of cross-dataset benchmarks and highlights the hidden mathematical discrepancies that are present in generative deepfake models.

V. COMPARATIVE *ANALYSIS*

Tool / Framework	Methodology	Primary Deployment	Security Focus	Core Target Layer
Amazon Rekognition	Temporal / Motion Video Analysis	Cloud (SaaS)	Enterprise Scalability	Video Pipeline / Sensor
SpoofSense	Micro-texture Analysis	API / Cloud	Single-Frame Low-Latency	Sensor (Epidermal Layer)
Oz Liveness	Deep Neural Nets / Reflection	On-Prem / Cloud	Regulatory Compliance	Environmental / 3D Mask
InsightFace	Feature Extraction (InspireFace)	Edge / IoT	Low Latency & Privacy	Local Device Processor
Silent-Face-AS	Lightweight CNN	Mobile / Edge	2D Replay Prevention	Mobile Sensor Layer
DeepFace	Modular Framework / Wrapper	Local / Research	Academic Baseline	Pipeline Customization
Swin Transformer V2	Hierarchical Self-Attention	Server / Cloud	Deepfake / Synthetic Media	Digital / Synthesis Layer

VI. DISCUSSION *AND OPEN CHALLENGES*

Modern FAS systems have proven to be very reliable in the face of attacks from a single source, but the combination of physical and digital attacks is a continuous challenge. While enterprise tools are good at detecting physical artifacts (surface reflection, edge detection, etc.), they often miss detection of deepfakes that are directly injected through software without going through the optical sensor. However, digital anomaly detection systems are generally not optimized for the low power edge devices. The engineering challenge of achieving optimal performance in terms of low HTER and low computational overhead still remains the main challenge.

VII. CONCLUSION AND FUTURE DIRECTIONS

There is an urgent need to transition towards multimodal and adaptive learning architectures in the context of the evolution of synthetic media. Future biometric systems need to shift from mere pixel-matching to "cognitive" facial understanding, that is, the understanding of micro-behaviors, pulse-regulated blood flow variations and multi-spectral sensor data. In an increasingly evolving landscape of digital identity threats, prioritising on-device processing will play a key role in slowing algorithmic bias, minimising data risk and providing a more secure and fair digital identity experience.

REFERENCES

[1] ISO/IEC, "Biometric presentation attack detection — Part 3: Testing and reporting," ISO/IEC 30107-3:2023, 2023.
[2] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, "Joint face detection and alignment using multitask cascaded convolutional networks," IEEE Signal Processing Letters, vol. 23, no. 10, pp. 1499-1503, 2016.
[3] R. Ramachandra and C. Busch, "Presentation attack detection methods for face recognition systems: A comprehensive survey," ACM Computing Surveys, vol. 50, no. 1, pp. 1-37, 2017.
[4] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, "Deepfakes and beyond: A survey of face manipulation and fake detection," Information Fusion, vol. 64, pp. 131-148, 2020.
[5] Z. Yu, Y. Qin, X. Li, C. Zhao, Z. Lei, and G. Zhao, "Deep learning for face anti-spoofing: A survey," IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI), vol. 45, no. 5, pp. 5609-5631, 2023.
[6] H. Xing, S. Y. Tan, F. Qamar, and Y. Jiao, "Face anti-spoofing based on deep learning: A comprehensive survey," Applied Sciences, vol. 15, no. 12, p. 6891, 2025.
[7] K. Patel, H. Han, and A. K. Jain, "Secure face unlock: Spoof detection on smartphones," IEEE Transactions on Information Forensics and Security, vol. 11, no. 10, pp. 2268-2283, 2016.
[8] S. Bhattacharjee, A. Mohammadi, and S. Marcel, "Spoofing Deep Face Recognition with Custom Silicone Masks," in Proc. IEEE International Conference on Biometrics Theory, Applications and Systems (BTAS), 2018, pp. 1-7.
[9] A. Rössler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Nießner, "FaceForensics++: Learning to detect manipulated facial images," in Proc. IEEE/CVF International Conference on Computer Vision (ICCV), 2019, pp. 1-11.
[10] Y. Li, X. Yang, P. Sun, H. Qi, and S. Lyu, "Celeb-DF: A large-scale challenging dataset for deepfake forensics," in Proc. IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2020, pp. 3207-3216.
[11] S. M. Ibrahim, M. S. Ibrahim, S. Khan, Y. W. Ko, and J. G. Lee, "Improving face presentation attack detection through deformable convolution and transfer learning," IEEE Access, vol. 13, pp. 31228-31238, 2025.
[12] Oloid AI, "Liveness detection guide: Protecting digital identity 2026," Whitepaper, Jan. 2026.
[13] ID-Pal, "Biometric liveness detection explained for 2026," Technical Report, Feb. 2026.
[14] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive Angular Margin Loss for Deep Face Recognition," in Proc. IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2019, pp. 4690-4699.
[15] Y. Liu, A. Jourabloo, and X. Liu, "Learning deep models for face anti-spoofing: Binary or auxiliary supervision," in Proc. IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2018, pp. 389-398.