



Comprehensive Survey Of Face Spoofing Detection: Methods, Datasets, Results, Challenges And Future Directions

¹Pratik Soni

¹Asst. Prof.

¹Department of Information Technology, MBIT

¹The CVM University, V.V.Nagar, INDIA

Abstract : Face recognition systems are widely used in mobile authentication, banking, surveillance, and security applications. However, they remain vulnerable to presentation attacks (spoofing), such as printed photos, replayed videos, and 2D/3D masks. This extended survey reviews classical and modern approaches for face anti-spoofing (FAS), covering hand-crafted methods, hardware/multi-modal solutions, and deep learning techniques. Public datasets, evaluation metrics, and comparative results are summarized. Diagrams illustrate spoofing attack taxonomy and FAS pipelines. We also discuss challenges such as generalization and deepfake detection, and conclude with promising directions for robust, explainable, and privacy-preserving FAS.

IndexTerms - Face Spoofing Mechanism, Presentation Attack, Authentication, Multi-Modal Solutions, DeepFake Detection, Quality Measures

I. INTRODUCTION

Biometric authentication has become a cornerstone of modern security systems, with facial recognition emerging as one of the most prominent modalities due to its convenience, non-intrusiveness, and wide range of applications [1]. From smartphone unlocking to airport security and financial transactions, face recognition systems are increasingly deployed in real-world scenarios. However, their widespread adoption has also revealed significant vulnerabilities to presentation attacks (PAs), commonly referred to as face spoofing. In such attacks, adversaries attempt to bypass recognition systems using printed photos, replayed videos, 3D masks, or even AI-generated synthetic faces [2]. These threats undermine the trustworthiness of face recognition systems and highlight the critical need for robust face anti-spoofing (FAS) mechanisms.

Face spoofing detection has thus emerged as a key research domain aimed at distinguishing genuine facial traits from fraudulent attempts [3]. Early methods primarily relied on handcrafted features such as texture descriptors (e.g., LBP, HOG) and motion cues to capture differences between real and spoofed faces [4]. While effective in controlled settings, these approaches struggled in unconstrained environments with variations in lighting, pose, and spoofing mediums. The advent of deep learning has significantly advanced the field, enabling models to learn discriminative spatial-temporal features directly from data [5]. Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and more recently, Vision Transformers have shown promising performance in detecting diverse attack types [6]. Nevertheless, challenges such as cross-dataset generalization, robustness to unseen attack types, and the demand for large annotated datasets continue to limit their practical deployment [7].

This survey provides a comprehensive overview of the current progress in face spoofing detection, systematically analyzing both traditional and deep learning-based approaches. It also examines publicly available datasets, evaluation protocols, and performance benchmarks widely adopted in the research community [8]. Furthermore, the paper discusses open challenges such as domain adaptation, multimodal fusion, and real-time detection, which remain unsolved in practical applications [9]. By consolidating recent advancements and identifying gaps, this survey aims to guide future research directions toward developing more reliable, secure, and generalizable FAS systems [10].

The print-attack database is introduced [3], featuring a motion-based algorithm to detect correlations between head movements and scenes, aiming to address this gap and enhance face recognition security. while the problem of spoofing detection comes from a texture analysis approach based on multi-scale local binary patterns that identifies live people versus face prints but also provides features usable for face recognition without user cooperation [4]. further extended the exploration to dynamic texture for detecting face spoofing and to learn the structure and dynamics of the facial micro-textures that characterise only real faces but not fake ones.

II. FACE SPOOFING METHODS

The term "face spoofing" describes the employment of deceitful techniques to mislead facial recognition software into granting unapproved or fraudulent access. The potential of face spoofing becomes a major problem as facial recognition technology becomes more widely used in many applications, such as mobile devices, security systems, and authentication procedures. Face spoofing is achieved using a variety of techniques, which can be divided into four categories: physical attacks, morphing attacks, multimodal attacks, and deepfake generation.

A. Physical Attacks

1) Print Attack: In a print attack, an attacker uses a high-resolution photograph of the legitimate user's face to impersonate and gain unauthorized access. This method is simple and often effective, especially if the facial recognition system lacks antispoofing measures.

2) Replay Attack: In a replay attack, the attacker records a video or captures facial data during a legitimate authentication session. They then replay this pre-recorded data to the facial recognition system during subsequent login attempts, tricking the system into granting access.

3) 3D Mask Attack: This involves the creation of a physical three-dimensional mask of the legitimate user's face. Advanced 3D printing technology allows attackers to produce realistic masks that mimic the contours and features of a real face, enabling successful spoofing.

B. Deepfake Generation (GAN-based Spoofing)

In order to produce realistic synthetic content, such as deepfake movies for face spoofing, Generative Adversarial Networks, or GANs, are extremely effective techniques. Generating artificial data and discriminating between actual and fake data are the two main components of GANs. Facial recognition algorithms find it difficult to distinguish between phone and authentic identities when faced with face spoofing since GANs can be trained to produce realistic facial pictures or movies.

C. Morphing Attack (Face Morphing Attack)

Attacks known as morphing includes merging features from several faces to generate a composite image. It is challenging for face recognition algorithms to correctly identify the person because the resulting morphing image combines features from both individuals. Using this technique, attackers might be able generate a false identity that is able to get by authentication checks.

D. Multimodal Attack

- 1) Mask Attack: In a mask attack, an attacker wears a physical mask resembling the face of an authorized user. This can be combined with other methods, such as voice impersonation, to enhance the effectiveness of the attack.
- 2) Texture and Pattern Attack: Attackers may use textured materials or patterns on a mask or other spoofing medium to deceive facial recognition systems. These textures can confuse algorithms by introducing elements that resemble genuine facial features.

III. FACE ANTI SPOOFING MECHANISM

Face anti-spoofing techniques use several types of approaches to identify and prevent face spoofing attacks, in which attackers trick facial recognition systems with images, videos, or other media. Based on the features they use, their type of analysis (dynamic or static), and the underlying technologies used, these approaches can be broadly defined.

- 1) Feature-based Techniques: In order to differentiate real faces from fakes, feature-based face anti-spoofing systems emphasis on identifying specific features from facial photos. Texture analysis is a popular method that looks for consistency in the patterns and imperfections in the skin's texture. Additionally, colour information is employed, examining differences in colour contrasts and patterns to find irregularities suggestive of spoofing attempts. Further, the term "liveness detection" refers to techniques used to identify indicators of life, such as head movement or eye blinking, frequently using additional sensors, such as depth or infrared ones, to improve accuracy. A key component of feature-based approaches is spectral analysis, which looks at face features in several frequency bands to spot unusual events.
- 2) Motion-based Techniques: In order to detect irregularities motion-based face antispoofing systems investigate temporal features of facial dynamics. By focusing on the temporal variations in facial characteristics, dynamic texture analysis can identify deviations in motion patterns that might point to a spoofing effort. By utilising the differences between real and artificial facial dynamics, facial dynamics analysis analyses how people's faces move and express themselves across time. Another method uses optical flow analysis to look for abnormal patterns produced on by face spoofing attacks by observing the flow of pixels between successive frames.
- 3) 3D-based Techniques: These techniques leverage three-dimensional information to enhance face anti-spoofing capabilities. Depth information from 3D sensors is utilized to distinguish between real and fake faces by exploiting differences in facial feature depth. 3D face reconstruction techniques go further by creating a three-dimensional model of the face, enabling the analysis of spatial structure and identification of anomalies in facial geometry. These methods contribute an additional layer of sophistication to anti-spoofing systems.
- 4) Machine Learning-based techniques: Machine learning plays a pivotal role in face antispoofing, with various supervised and deep learning methods being employed. Supervised learning involves training models on labelled datasets containing both genuine and fake face samples. Popular algorithms include support vector machines (SVM), random forests, and neural networks. Deep learning, utilizing architectures such as convolutional neural networks and recurrent neural networks, enables automated feature learning and extraction. Transfer learning adapts pre-trained models from general face recognition tasks for face anti-spoofing, enhancing performance with fine-tuning on specific datasets.
- 5) Multimodal Fusion Techniques: Multimodal fusion techniques integrate information from multiple sources to improve overall anti-spoofing accuracy. This may involve combining RGB images with depth maps, infrared data, or other modalities. By leveraging complementary information, these techniques enhance the robustness of antispoofing systems, providing a more comprehensive understanding of the presented facial data.

6) Biometric Fusion Techniques: Biometric fusion techniques combine face anti-spoofing with traditional face recognition systems or other biometric modalities. Fusion with face recognition enhances security by combining liveness detection with identity verification. Voice and speech analysis may also be incorporated to create multimodal biometric systems, adding additional layers of security and making the overall system more resilient to spoofing attempts.

7) Traditional Computer Vision Techniques: Traditional computer vision techniques are employed in face anti-spoofing to address specific aspects of image analysis. Edge detection, for instance, focuses on identifying boundaries between facial features by examining edge patterns, while histogram analysis evaluates pixel intensity distributions for irregularities. These techniques provide classical yet effective approaches to antispoofing.

8) Hybrid Techniques: Hybrid techniques involve combining methodologies from different categories to create robust antispoofing systems. By integrating the strengths of multiple approaches, these hybrid techniques aim to improve overall performance and detection capabilities. The combination of feature extraction, motion analysis, and machine learning, for example, creates a comprehensive approach capable of detecting a wide range of face spoofing attacks. Researchers often experiment with hybrid models to achieve a balance between accuracy and computational efficiency in real-world scenarios.

IV. LITERATURE SURVEY

This comprehensive study aims to provide an overview of the existing works and approaches in the field of face spoofing detection. A lot of work has been done in this field, including:

Enoch Solomon and Krzysztof J. Cios 2023, [10] propose a face anti-spoofing system that integrates image quality features and deep learning methods. The system aims to distinguish between genuine and spoofed faces by analyzing both the inherent quality of the image and using deep learning models to learn discriminative representations. The combination of image quality features and deep learning enhances the system's ability to detect spoofing attacks, making it more robust and effective in real-world scenarios.

Deepika Sharma and Arvind selwal 2023, [11] provide a survey of the different techniques that have been proposed for face presentation attack detection (PAD). Pad is the task of detecting whether a face image or video is a genuine presentation of a person's face or a presentation attack. Presentation attacks can be carried out using a variety of methods, such as using printed images, masks, or even mobile phones. The paper concludes by discussing the future of pad. The authors believe that pad is an important research area, and that there is still much work to be done in developing effective pad techniques. They also believe that pad will become increasingly important as face recognition systems become more widely deployed.

L. Birla, P. Gupta, and S. Kumar 2023, [12] address the vulnerability of face analytic systems to face spoofing attacks in the digital world. The authors propose a face anti-spoofing method called SUNRISE (Short videos UsiNg pRe-emptive Split and mErge) that utilizes remote Photoplethysmography (rPPG) to detect cardiovascular signals and mitigate face spoofing attacks. However, they acknowledge that the performance of rPPG-based anti-spoofing methods can be degraded due to illumination variation and face deformations, even with longer-duration face videos. To overcome this limitation, SUNRISE introduces a split and merge mechanism.

Xin Cheng et al., [13] propose an anti-spoofing method for facial recognition systems in the Internet of Things (IoT) environment. It introduces a spoofing-detection algorithm based on optical flow and texture features, utilizing a two-channel convolutional neural network (CNN) to extract and fuse facial characteristics. To enhance the optical flow field map with liveness information, a motion amplification algorithm is applied. The method was evaluated on the Replay Attack dataset, achieving a half total error

rate of 0.66%. By effectively discerning real and fake faces, this approach enhances the security and reliability of facial recognition systems, making it a promising solution for combating face spoofing attacks in IoT applications.

Shizhe Zhang and Wenhui Nie 2023

[14] introduce a novel approach called Multi-Domain Feature Alignment Framework (MADG) for face anti-spoofing, which enhances the robustness of face recognition systems against presentation attacks. Existing methods face challenges in generalizing features across different domains due to distribution discrepancies. MADG addresses this issue by employing an adversarial learning process to align features from multiple source domains, narrowing the domain differences. Additionally, a multi-directional triplet loss is incorporated to improve the separation between real and fake faces in the feature space. Extensive experiments on public datasets demonstrate that MADG outperforms current state-of-the-art methods, proving its effectiveness in face anti-spoofing.

Z. Kong et al. 2023, [15] address the challenge of generalizing presentation attack detection (PAD) techniques to unknown presentation attack instruments (PAIs). It highlights the importance of model initialization for generalization, which is often overlooked. To improve generalization, the paper proposes a self-supervised learning-based method called DF-DM. This method leverages a global-local view and employs de-folding and de-mixing techniques to derive task-specific representations for PAD. During de-folding, region-specific features are learned to represent samples in a local pattern, while de-mixing drives detectors to obtain instance-specific features with global information for more comprehensive representation. The proposed DF-DM method outperforms state-of-the-art methods in face and fingerprint PAD tasks on more complex and hybrid datasets, achieving a significant reduction in equal error rate (EER).

Yousef Atoum, Yaojie Liu, Amin Jourabloo, and Xiaoming Liu 2017, [17] present a novel approach for detecting face spoofing attacks. By utilizing patch-based and depth-based convolutional neural networks (CNNs), the method effectively combines local texture information and geometric cues to distinguish between genuine and fake faces. Extensive evaluations on publicly available datasets demonstrate the superiority of their approach over existing methods, showcasing its improved accuracy and robustness in detecting various spoofing attacks. The proposed technique represents a significant contribution to enhancing the security and reliability of face recognition systems by effectively countering face spoofing threats.

Chien-Yi Wang, Yujiang Lu, S. Lai, [18] present a straightforward yet effective approach for detecting face spoofing attacks. The proposed framework, PatchNet, focuses on fine-grained patch recognition within the face region. It extracts small patches from the face and classifies them as genuine or spoofed based on their distinctive features. By focusing on fine-grained details, the method aims to capture subtle cues that differentiate between real and fake faces. The paper demonstrates the efficacy of PatchNet in detecting spoof attacks through evaluations on publicly available face anti-spoofing datasets. Its simplicity and computational efficiency make it a promising approach for real-world face recognition security applications.

V.RELATED RESULTS AND DISCUSSION

The experimental results clearly demonstrate the evolution of face anti-spoofing detection methods from traditional handcrafted features toward deep learning approaches. Early techniques, such as LBP-TOP and DoG+SVM, achieved moderate performance on datasets like CASIA-FASD and Replay-Attack, with error rates exceeding 12–15%. While these methods provided important baselines and highlighted the feasibility of spoofing detection, their limitations became evident under real-world conditions involving variations in illumination, pose, and spoofing mediums. For example, the LBP-TOP method reported an Equal Error Rate (EER) of 15.2% on CASIA-FASD, showing that handcrafted descriptors alone struggled to capture subtle discriminative features between genuine and spoofed faces.

With the introduction of deep learning, performance significantly improved across multiple benchmark datasets. CNN-based models on MSU-MFSD achieved accuracy above 96%, while more advanced architectures such as ResNet-50 and MobileNet reduced the Average Classification Error Rate (ACER) and Half Total Error Rate (HTER) to below 5% on OULU-NPU and SiW, respectively. More recent methods, including Vision Transformers, have pushed the boundaries further, achieving up to 99% accuracy on large-scale datasets like CelebA-Spoof. These results highlight the superiority of deep feature representations over handcrafted ones, as well as the rapid progress of the field. However, the variations in performance across datasets also indicate persistent challenges in generalization and robustness, especially against unseen attack types.

Table 1 Results

Method	Dataset	Metric	Result
LBP-TOP [2014]	CASIA-FASD	EER	15.20 %
Motion Magnitude [2015]	Replay-Attack	HTER	12.70 %
CNN (2017)	MSU-MFSD	Accurac y	96.40 %
ResNet-50 (2019)	OULU-NPU	ACER	4.20%
Vision Transformer (2022)	CelebA-Spoof	Accurac y	99.10 %

The comparative results of face anti-spoofing detection methods indicate a clear progression from handcrafted feature-based approaches to deep learning architectures. While traditional methods such as LBP-TOP and motion analysis established important baselines, their higher error rates demonstrate limited robustness in unconstrained environments. Deep learning models, including CNNs, ResNet variants, and MobileNet, have significantly reduced error rates and achieved higher accuracy across benchmark datasets. More recently, Vision Transformers and large-scale pretraining strategies have further improved detection performance, achieving near-perfect accuracy in some cases. Despite this progress, cross-dataset performance remains a critical challenge, suggesting that current methods are still prone to overfitting to specific attack types and environments.

Future research should focus on enhancing generalization and robustness to unseen spoofing scenarios, such as novel presentation attacks generated using advanced AI techniques. Multimodal fusion, combining visual cues with depth, thermal, or remote physiological signals, offers promising directions to strengthen security. Additionally, lightweight architectures and model optimization will be essential for real-time deployment on mobile and embedded devices. Finally, establishing standardized benchmarks and large-scale diverse datasets will remain key to ensuring fair evaluation and guiding the development of next-generation face anti-spoofing systems capable of withstanding increasingly sophisticated threats..

VI. ACKNOWLEDGMENT

I herewith thank to Guru Hari HariPrasad Swamiji and Guru Hari Prabodhjivan Swamiji for their unconditional support and blessings. Also thank My wife and child for their constant support. Also thank all my Group Members.

REFERENCES

- [1] [1 Dong, Xiaoyi et al. "Protecting Celebrities from DeepFake with Identity Consistency Transformer." 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2022): 9458-9468.
- [2] Anthony, Peter et al. "A Review of Face Anti-spoofing Methods for Face Recognition Systems." 2021 International Conference on INnovations in Intelligent SysTems and Applications (INISTA) (2021): 1-9.
- [3] Anjos, André, and Sébastien Marcel. "Counter-measures to photo attacks in face recognition: A public database and a baseline." 2011 International Joint Conference on Biometrics (IJCB) (2011): 1–7.
- [4] Määttä, Jukka et al. "Face spoofing detection from single images using micro-texture analysis." 2011 International Joint Conference on Biometrics (IJCB) (2011): 1-7.
- [5] Komulainen, Jukka et al. "Face Spoofing Detection Using Dynamic Texture." ACCV Workshops (2012).
- [6] Zhang, Zhiwei et al. "A face antispoofing database with diverse attacks." 2012 5th IAPR International Conference on Biometrics (ICB) (2012): 26-31.
- [7] Chen, Cunjian et al. "Spoofing faces using makeup: An investigative study." 2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA) (2017): 1-8.
- [8] Mou, Lichao et al. "Learning Spectral-Spatial-Temporal Features via a Recurrent Convolutional Neural Network for Change Detection in Multispectral Imagery." IEEE Transactions on Geoscience and Remote Sensing 57 (2018): 924-935.
- [9] Muhammad, Usman et al. "Deep Ensemble Learning with Frame Skipping for Face Anti-Spoofing." 2023 Twelfth International Conference on Image Processing Theory, Tools and Applications (IPTA) (2023): 1-6.
- [10] Solomon, Enoch & Cios, Krzysztof. (2023). FASS: Face Anti-Spoofing System Using Image Quality Features and Deep Learning. Electronics. 12.2199.10.3390/electronics12102199.
- [11] [11] Sharma, Deepika & Selwal, Arvind. (2023). A survey on face presentation attack detection mechanisms: hitherto and future perspectives. Multimedia Systems. 29. 1-51. 10.1007/s00530-023-01070-5.
- [12] L. Birla, P. Gupta and S. Kumar, "SUNRISE: Improving 3D Mask Face Anti-Spoofing for Short Videos Using Pre-Emptive Split and Merge," in IEEE
- [13] Transactions on Dependable and Secure Computing, vol. 20, no. 3, pp. 1927-1940, 1 May-June 2023, doi: 10.1109/TDSC.2022.3168345.
- [14] Xin Cheng, Jingmei Zhou, Xiangmo Zhao, Hongfei Wang, and Yuqi Li. 2023. A presentation attack detection network based on dynamic convolution and multilevel feature fusion with security and reliability. Future Gener. Comput. Syst. 146, C (Sep 2023), 114–121. <https://doi.org/10.1016/j.future.2023.04.012>
- [15] Zhang S, Nie W. Multi-Domain Feature Alignment for Face Anti-Spoofing. Sensors. 2023; 23(8):4077. <https://doi.org/10.3390/s23084077>
- [16] Z. Kong et al., "Taming Self-Supervised Learning for Presentation Attack Detection: De-Folding and De-Mixing," in IEEE Transactions on Neural Networks and Learning Systems, doi: 10.1109/TNNLS.2023.3243229.

- [17] Li, C., Li, Z., Sun, J. et al. Middle-shallow feature aggregation in multimodality for face anti-spoofing. *Sci Rep* 13, 9870 (2023). <https://doi.org/10.1038/s41598-023-36636-w>
- [18] Yousef Atoum, Yaojie Liu, Amin Jourabloo, and Xiaoming Liu. Face anti-spoofing using patch and depth-based cnns. In 2017 IEEE International Joint Conference on Biometrics (IJCB), pages 319–328, 2017.
- [19] Chien-Yi Wang, Yujiang Lu, S. Lai. "PatchNet: A Simple Face Anti-Spoofing Framework via Fine-Grained Patch Recognition." *Computer Science*. In Proceedings of the 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 27 March 2022.
- [20] A. George and S. Marcel, "Deep Pixel-wise Binary Supervision for Face Presentation Attack Detection," 2019 International Conference on Biometrics (ICB), Crete, Greece, 2019, pp. 1-8, doi: 10.1109/ICB45273.2019.8987370.
- [21] Günay Yılmaz, Asuman & Turhal, Ugur & Nabiyeu, Vasif. (2023). Face presentation attack detection performances of facial regions with multi-block LBP features. *Multimedia Tools and Applications*. 1-25. 10.1007/s11042-023-14453-7.