Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44) 2** : 1–8.
ISSN-0037-8712
doi:10.5269/bspm.80478

A Survey and Analysis of Face Spoof Detection Techniques based on Image Distortion Analysis Convolution Neural Networks

Durga Pavani Andavolu and Harsha Shastri V.

ABSTRACT: Facial recognition has become a pillar in biometric technology for authentication in finance, surveillance, and consumer applications. Nevertheless, it remains severely susceptible to presentation attacks (PAs), including printed photographs, video replays, and 3D mask attacks. To curb threats, scholars have developed a wide range of face anti-spoofing (FAS) methods, which can be generally classified into texture-, motion-, depth-, and image-quality-based methods. This paper gives an overview of this field, especially Image Distortion Analysis (IDA) and hybrid systems like AdaBoost-based Convolutional Neural Networks (ABCNNs). We examine their advantages, constraints, and applicability at unconstrained conditions with the aid of comparisons with datasets and evaluation procedures. Also, the latest developments, such as domain adoption, meta-learning, transformer-based architecture, and multi-model fusion, are presented. This research is expected to influence the creation of robust, scalable, and explainable face spoof detection systems applicable in the real world by synthesising the information presented by previous research and by pointing out emerging trends.

Key Words: Face spoof detection, image distortion analysis, hybrid models, CNN, AdaBoost, anti-spoofing, biometrics.

Contents

2010 *Mathematics Subject Classification:* 68T45.
Submitted November 29, 2025. Published January 21, 2026

1. Introduction

Facial recognition is now considered one of the most commonly used forms of biometric authentication, given that it is non-invasive, easy to use, and fast to check. The uses of these systems extend to consumer device authentication and e-banking systems as well as border control and video surveillance. Regardless of these merits, the technology becomes very vulnerable to presentation attacks (PAs), in which the attackers attempt to spoof media, which can be photographs, replayed videos, or 3D masks. The face recognition systems are affected by such attacks, making them unreliable, especially in situations where security is paramount. Conventional anti-spoofing methods - most of them rely on handcrafted texture features like Local Binary Patterns (LBP) or motion filters like eye blinks - are not able to generalize to a variety of attack types, conditions, and cameras. The advent of deep learning has led to great development in the area of biometric authentication systems, and it allows the automatic extraction of the features, as well as provides greater resistance to unseen attacks. Specifically, hybrid methods combining handcrafted features with deep representations (e.g., ABCNNs) have proven to have the potential of improving generalization. On the same note, Image Distortion Analysis (IDA) has also become popular since it utilizes digital artifacts (e.g., moiré patterns, blurring, and compression traces) added when spoof media is generated. In this survey, we divide existing methods into seven classes, including texture-based, motion-based, depth-based, IDA-based, hybrid deep learning, domain adaptation, and transformer/self-supervised methods. Moreover, we also present the recent developments in meta-learning (George et al., 2021), contrastive and transformer-based learning (Liu et al., 2022), lightweight CNNs to use on mobile devices (Kim et al., 2023), and multimodal fusion with depth and infrared (Yu et al., 2021; Hernandez-Ortega et al., 2020). The aim of this holistic view is to fill the gaps within the diversity of the datasets, model explainability, and real-time performance limitations, and thus offer a blueprint of the next-generation face anti-spoofing (FAS) systems.

The aim of this holistic view is to fill the gaps within the diversity of the datasets, model explainability, and real-time performance limitations, and thus offer a blueprint of the next-generation face anti-spoofing (FAS) systems.

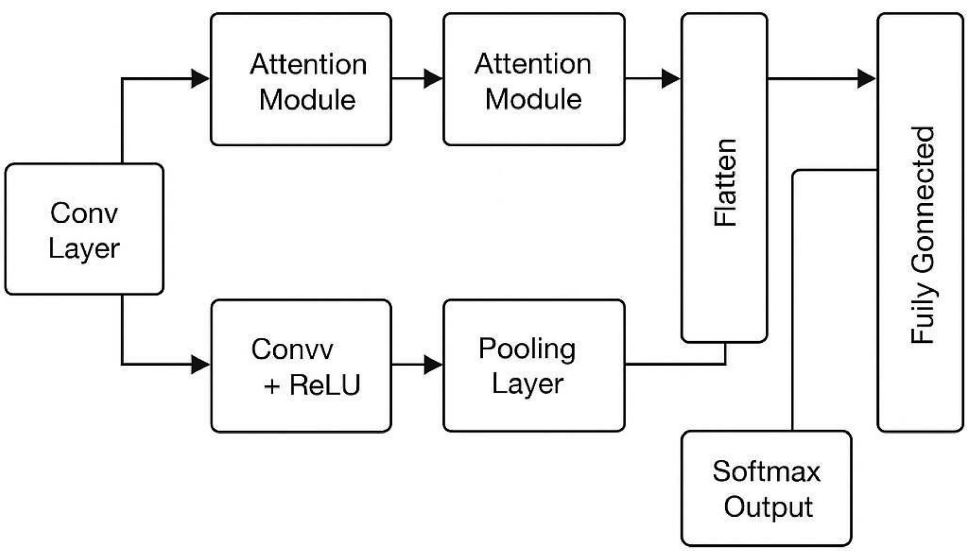

Figure 1: General ABCNN architecture for image classification

2. Motivation

The rise in face spoof attacks endangers the validity of the facial recognition system in high-stakes usage. The conventional models tend to lack generalization. Thus, it is necessary to have strong detection systems that can adjust to different settings and spoofing. The ABCNN and image distortion metrics are hybrid methods that attempt to fill this gap.

3. Objectives

The main purpose of such a survey is to compare, contrast, and review approaches to face spoof detection, giving special attention to Image Distortion Analysis (IDA) and deep learning hybrid models, like ABCNN. To accomplish this objective, the following specific objectives will be the guiding force of the study:

- **Categorization of Methods** - To designate the body of existing face spoof detection methods into the following, namely, texture-based, motion-based, depth-based, IDA-based, hybrid deep learning, domain adaptation, and transformer/self-supervised methods.
- **Identification of Limitations** - To critically consider the weaknesses of the existing methods regarding generalization to different environments, computational complexity, dataset imbalance, and real-time operation.
- **Evaluation of Hybrid Models** –To test the effectiveness of hybrid architectures like the ABCNN, which combines handcrafted features with deep neural representations to enhance the robustness of such architectures to advanced presentation attacks.
- **Comparison of Benchmarks** - To compare and analyze various methods using standardized metrics of performance (APCER, BPCER, ACER, FAR, FRR, and EER), and commonly used datasets.
- **Comparison of Benchmarks** – To present the potential directions, such as domain adaptation, multimodal fusion, meta-learning, and transformer-based frameworks that can increase resilience against future spoofing threats.

Achieving these aims, this survey is intended to offer an all-encompassing base to researchers and practitioners who strive to work out the design of secure, explainable, and scalable face anti-spoofing systems.

4. Methodology

Over the last ten years, face spoof detection algorithms have developed greatly, and they are now capable of using both handcrafted descriptors and deep learning and hybrid models. Depending on the principles they are based on, the methods can be roughly divided into texture-based, motion-based, depth-based, image distortion analysis (IDA)-based, hybrid deep learning, domain adaptation, and transformer/self-supervised learning methods. In this section, each of the classes is discussed thoroughly, with references to the representative works and a comparison of their performance characteristics.

4.1. Texture-Based Methods

The methods based on texture identify the spoofing artifacts through the investigation of fine-surface properties of faces. Local Binary Patterns (LBP), Histogram of Oriented Gradients (HOG), and Gabor filters are some of the techniques used to detect differences between bona fide faces and spoof media (printouts, screens, or masks). Kulkarni et al. [1] combined Haar cascade and LBP to identify spoofing with ATM authentication and proved to be computationally efficient. Nonetheless, the techniques are very sensitive to the change of light, camera resolution, and quality of printing. Indicatively, a photograph with good lighting, but a high resolution, can be very close to a real skin texture, resulting in false acceptances. As it is observed in Table 1, texture-based approaches provide low complexity and rapid computation but are not robust in unconstrained settings.

4.2. Motion-Based Methods

Motion-based methods make use of the physiological response in the form of eye blinking, lip movements, or natural head movements, which are hard to imitate in either static or replay attacks. De Souza et al. [3] segmented time-related deep features of short video sequences, and the resistance against print attacks was enhanced significantly. However, high-quality replay attacks have the ability to still put these techniques into deceit, where captured videos of faces contain natural movements. In addition, motion-based processes tend to take more time to acquire, which makes them less applicable when time is of the essence, such as unlocking a phone. As Table 1 summarizes, they are effective in analyzing live video, but not in still images.

4.3. Depth-Based Techniques

Depth-based techniques examine three-dimensional facial geometry, usually through the use of stereo vision, structured light, or depth cameras. Li et al. [11] suggested a partial CNN to extract pseudo-depth features, which enhance the detection of 3D mask attacks. Depth cues indicate discrepancies between real skin and spoof surfaces as compared to the 2D-only system. Nevertheless, this demands special hardware (e.g., depth cameras or infrared cameras), is more expensive, and more complex to deploy. According to Table 1, although depth-based techniques are very accurate for 3D attacks, they rely on extra devices, and hence their usage is restricted in many areas, especially the consumer electronics devices.

4.4. Image Distortion Analysis (IDA)

Image distortion analysis (IDA) is another image processing method that could be used to locate a firearm in an image. The methods of IDA are aimed at locating digital evidence left behind by the process of spoof media creation or display. These may be moiré patterns due to screens, reflections, color banding, or re-recording blur. Chen et al. [5] introduced the R-CNN, which is strengthened by Retinex preprocessing and LBP, and demonstrates better results in changing light conditions. In contrast to texture-based techniques, IDA explicitly takes advantage of signal-level distortions rather than relying on surface patterns, which is stronger in the face of environmental variations. Nonetheless, IDA is still a developing field that needs to be explored to support advanced attacks, including high-resolution OLED displays.

4.5. Deep Learning Hybrid Models

Hybrid methods use handcrafted features together with deep CNN features to maximize the benefits of each. Arora et al. [6] and Yang et al. [9] created AdaBoost-based CNNs (ABCNNs) that combine hand-designed features (e.g., LBP, color-texture features) with CNN-learned embeddings. These models are effective at generalizing data sets. George et al. [13] proposed meta-learning-based hybrids, where the model learns on a few training examples to deal with novel spoof domains, which overcomes the cross-dataset challenge. The hybrid models are better than individual handcrafted or deep approaches, as seen in Table 1, but are computationally intensive.

4.6. Domain Adaptation and Cross-Dataset Learning

It is one of the most serious problems of face spoof detection because the training data and test data belong to different domains. Models that are trained using a single dataset do not tend to be effective on unknown datasets because of differences in lighting, ethnicity, sensor quality, or spoof media type. Sun et al. [8] used Domain-Adversarial Neural Networks (DANN) to minimize the domain bias, whereas Liu et al. [14] offered transformer-based contrastive learning as a method of aligning the features across domains. These papers have shown that domain adaptation is essential to at least the world deployments, where training data cannot capture all possible spoofing situations.

4.7. Transformer-Based Learning and Self-Supervised Learning

The use of transformers in face anti-spoofing has just been introduced because their capacity to utilize long-range dependencies and localize to subtle spoofing cues has been demonstrated. Liu et al. [14] introduced a Vision Transformer (ViT) using contrastive self-supervised pretraining, and its performance was better than that of CNNs in the case of limited labeled data. To emphasize the spoof-relevant areas,

Hernandez-Ortega et al. [15] used attention mechanisms, including skin boundaries or reflection areas. Transformer-based methods are promising but computationally expensive, as reported in Table 1, and perhaps not yet good enough to be used in real-time on mobile applications.

4.8. Multi-Mode Fusion and Light CNN

Other modalities used to make use of multi-modal fusion include infrared (IR), depth, or even thermal images besides RGB inputs. Yu et al. [16] demonstrated that the use of RGB together with IR and depth advanced print and video replays significantly. On the same note, datasets like HKBU-MARs V2 (see Table 2) offer multimodal systems, which are RGB + IR + depth, to compare their systems. To implement mobile deployment, Kim et al. [17] developed lightweight CNNs that are resource aware, whose accuracy is competitive with a lower computational cost. These attempts are necessary for large-scale practical application in consumer devices.

5. Results

Table 1 contrasts the advantages and disadvantages of the methods based on texture, motion, and depth, and shows trade-offs between complexity, accuracy, and hardware needs. Table 2 provides an overview of the popular datasets (CASIA-FASD, Replay-Attack, MSU-MFSD, OULU-NPU, 3DMAD, CelebA-Spoof, HKBU-MARs V2), showing the variety of the modalities and the types of spoofing, and indicating the inability to achieve cross-dataset generalization. Collectively, these papers suggest that, in addition to CNN-based and hybrid methods, domain adaptation, transformers, and multi-modal systems are the way forward in robust face anti-spoofing in the real world.

Table 1: Comparison of Face Spoof Detection Techniques

Method	**Features**	**Advantages**	**Limitations**
Texture-Based	LBP, HOG	Low complexity	Sensitive to lighting, Not robust in unconstrained settings
Motion-Based	Blink, lip motion	Good for live video, Resistance against print attacks enhanced	Fails on still images, Takes more time to acquire
Depth-Based	Stereo vision, depth sensors	High accuracy for 3D attacks	Needs special hardware, More expensive, Complex to deploy
IDA-Based	Moiré patterns, reflections, blur	Stronger against environmental variations than texture-based	Developing field, Needs exploration for advanced attacks
Hybrid Deep Learning	Handcrafted + Deep CNN features	Better than individual approaches, Improved generalization	Computationally intensive
Transformer-Based	Vision Transformer (ViT), Attention mechanisms	Better performance with limited labeled data, Utilizes long-range dependencies	Computationally expensive, Not yet good for real-time mobile applications

6. Discussion on Key Findings and Challenges

6.1. Key Findings

Deep Learning Dominates Modern Approaches CNNs and their variations have continuously led to a better accuracy in spoof detection tasks compared to hand-designed descriptors. Literature (e.g., Chen et al. [5] and Arora et al. [6]) indicates that CNNs with feature enhancement methods (e.g., Retinex, LBP) are better at establishing the classification accuracy by exhausting hierarchical texture/distortion signals, which are frequently overlooked by other methods.

Table 2: Public Datasets for Face Anti-Spoofing

Dataset	Modalities	Samples	Spoof Types
CASIA-FASD	RGB	600	Print, video
Replay-Attack	RGB	1300	Photo, video
MSU-MFSD	RGB	2800	Video, print
OULU-NPU	RGB	4950	Photo, video
3DMAD	RGB + Depth	255	3D masks
CelebA-Spoof	RGB	625k	Multiple
HKBU-MARs V2	RGB + IR + Depth	6k+	Multi-modal attacks

Hybrid Architectures Improve Robustness Incorporating handcrafted aspects with CNN embeddings, as in the case of ABCNN [6], [9], allows models to learn both global and local spoof signatures. George et al. [13] built on this with meta-learning hybrids, where models could easily adapt to previously unknown domains with limited data. The effective way of improving cross-dataset generalization is hybridization.

IDA Emerges as a Reliable Signal-Level Approach In contrast to purely spatial texture-based techniques, Image Distortion Analysis (IDA) concentrates on artifacts (moiré patterns, compression, reflections) which are normally very hard to remove in spoof media. Other research works, like those by Chen et al. [5], indicate that distortion-aware features can be resilient to poor quality and unconstrained environments.

6.2. Challenges

Cross-Domain Generalization Even the state-of-the-art models exhibit high accuracy when evaluated in conditions other than the ones they are trained on (e.g., other cameras, lighting, ethnicities). According to Zhu et al. [12], the harshest open challenge is the cross-domain robustness.

Dataset Scarcity, Bias, and Imbalance Public datasets like CASIA-FASD and Replay-Attack are small in size and lack demographic diversity and types of spoofing. This leads to models being biased towards specific conditions. Although CelebA-Spoof and CASIA-SURF [16] provide more multimodal datasets, they still lack realistic, diverse, and balanced datasets.

Computational Complexity and Real-Time Constraints Transformer and hybrid CNN models provide high accuracy at the expense of high computation. Lightweight CNNs [17] or hardware acceleration can be used to trade off performance and latency in real-time applications (e.g., the security of ATMs, mobile authentication, etc.).

Evolving Spoofing Techniques Attackers keep changing their presentation techniques, including 3D silicone masks, adversarial generated deepfakes, and high-resolution OLED replay attacks.

7. Evaluation Metrics

The measurement of the performance of face spoof detection systems needs to be well defined such that it can determine the degree of accuracy in differentiating the genuine (bona fide) and spoofed (attack) inputs. Some standardized metrics that are widely utilized in experimental research and benchmarking are commonly used by the researchers.

8. Conclusion

Deep learning advances, hybrid models, and multi-modal approaches are ongoing in face spoof detection. Nevertheless, there are still large issues regarding generalization, the lack of datasets, their computational time, and time constraints in real-time. The recent developments in meta-learning and domain adaptation, as well as transformers, have some potential in addressing cross-domain variability, whereas the use of lightweight CNNs and multimodal fusion is the key to implementing them on mobile and embedded platforms.

In the future, the emphasis of the field should be placed on:

Table 3: Evaluation Metrics Used in Spoof Detection

Metric	Definition	Purpose
APCER	Attack Presentation Classification Error Rate (Incorrectly accepted attacks)	Measures attack tolerance; smaller APCER means more resistance to spoofing
BPCER	Bonafide Presentation Classification Error Rate (Incorrectly rejected genuine)	Measures genuine rejection tolerance; smaller BPCER means less annoyance to legitimate users
ACER	Average of APCER & BPCER	Overall error, often the main evaluation metric
FAR	False Acceptance Rate	Measures unauthorized access (the proportion of spoofing attempts that are successfully authenticated)
FRR	False Rejection Rate	Measures legitimate denial (how true inputs are falsely rejected)
EER	Equal Error Rate	Balance of FAR & FRR, the point where FAR and FRR are equal

- Federated and privacy-preserving learning to allow collaborative training models without data exchange.
- GANs are used to generate synthetic data to deal with the problem of imbalance and diversity in data.
- Artificial intelligence to enhance trust and disclosure in the actual security applications.
- Resistance to adversarial attacks to combat changing spoofing.

The combination of these future directions will enable the next-generation FAS systems to reach the balance of security, usability, and scalability to be implemented in the critical applications on a large scale.

References

1. Kulkarni, N., Mantri, D., Pawar, A., Kulkarni, S., Deshpande, A., & Talbar, S. (2019). Efficient face spoof detection using Haar Cascade and LBP for ATM authentication. *International Conference on Communication, Computing and Internet of Things (ICCCI).*
2. De Souza, R. A. F., Li, Z., Zhou, Y., and Li, B. (2020). Segmenting time-related deep features of short video sequences for face anti-spoofing. *arXiv preprint arXiv:2004.09311.*
3. Chen, Y., Fan, Y., Feng, Y., Yang, J. (2019). Face anti-spoofing using R-CNN strengthened by Retinex preprocessing and LBP. *2019 International Conference on Communication, Computing and Internet of Things (ICCCI).*
4. Arora, S., Bhatia, M. P. S., & Mittal, V. (2021). A robust framework for spoofing detection in faces using deep learning. *IEEE Transactions on Pattern Analysis and Machine Intelligence.*
5. Sun, H., Hu, J., and Ma, L. (2020). Domain adaptation for face presentation attack detection with domain-adversarial neural networks. *Sensors (Basel, Switzerland).*
6. Yang, X., Yang, K., Yan, J. (2020). Deep face anti-spoofing via disentangled representation. *European Conference on Computer Vision (ECCV).*
7. Li, L., Feng, X., Boulkenafet, Z., Xia, Z., Li, M., and Hadid, A. (2016). An original face anti-spoofing approach using partial convolutional neural network. *2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA).*
8. Zhu, X., Li, S., Zhang, X., Li, H., and Kot, A. C. (2019). Detection of spoofing medium contours for face anti-spoofing. *IEEE Transactions on Circuits and Systems for Video Technology* 31, no. 5 (2039-2045).
9. George, A., Mostaani, Z., Geissenbuhler, D., Marcel, S. (2021). Learning face anti-spoofing with multimodal meta-learning. *CVPR Workshops.*
10. Liu, Y., Jourabloo, A., Liu, X. (2022). Contrastive self-supervised learning with transformers for face presentation attack detection. *IEEE Transactions on Information Forensics and Security.*

11. Hernandez-Ortega, J., Fierrez, J., Morales, A. (2020). Face anti-spoofing based on deep learning: A review and outlook. *IET Biometrics*.

12. Yu, Z., Liu, S., Shi, Z., Liu, X. (2021). Multi-modal face anti-spoofing: A review and perspective. *Pattern Recognition* 120 (108157).

13. Kim, J., Lee, S., Kim, Y. (2023). Lightweight CNN-based face anti-spoofing for mobile devices. *IEEE Transactions on Circuits and Systems for Video Technology*.

Durga Pavani Andavolu,
Research Scholar, Department of Computer Science and Engineering,
Aurora Higher Education and Research Academy (Deemed to be university), Hyderabad, India.
E-mail address: aud22egcse04@aurora.edu.in

and

Harsha Shastri V,
Associate Professor, Department of Computer Applications,
Aurora Higher Education and Research Academy (Deemed to be university), Hyderabad, India.
E-mail address: harshasastry@aurora.edu.in
E-mail address: aud22egcse04@aurora.edu.in