A review of state-of-the-art in face presentation attack detection: from early development to advanced deep learning and multi-modal fusion methods.

ABDULLAKUTTY, F., ELYAN, E. and JOHNSTON, P.

2021

A review of state-of-the-art in Face Presentation Attack Detection: from early development to advanced deep learning and multi-modal fusion methods

Faseela Abdullakutty*, Eyad Elyan, Pamela Johnston

School of Computing, Robert Gordon University, Aberdeen, United Kingdom

Abstract

Face Recognition is considered one of the most common biometric solutions these days and is widely used across a range of devices for various security purposes. The performance of FR systems has improved by orders of magnitude over the past decade. This is mainly due to the latest developments in computer vision and deep convolutional neural networks, and the availability of large training datasets. At the same time, these systems have been subject to various types of attacks. Presentation attacks are common, simple, and easy to implement. These simply involve presenting a video, photo, or mask to the camera or digital sensor and have proven capable of fooling FR systems and providing access to unauthorised users. Presentation attack detection is increasingly attracting more attention in the research community. A wide range of methods has already been developed to address this challenge. Deep learning-based methods in particular have shown very promising results. However, existing literature suggests that even with state-of-the-art methods, performance drops significantly in cross-dataset evaluation. We present a thorough, comprehensive, and technical review of existing literature on this timely and challenging problem. We first introduce and discuss the presentation attack problem and cover related and recent work in this area. In-depth technical details of existing presentation attack detection methods are then presented and critically discussed and evaluated, followed by a comprehensive discussion and evaluation of existing public datasets and

*Corresponding author

Email addresses: f.abdullakutty@rgu.ac.uk (Faseela Abdullakutty), e.elyan@rgu.ac.uk (Eyad Elyan), p.johnston2@rgu.ac.uk (Pamela Johnston)

commonly used evaluation metrics. Our review shows clearly that despite the recent and significant advances in this area of research, detecting unseen attacks is still considered a key problem. Machine learning methods tend to perform well, but only when test data comes from the same distribution as the training data (i.e. same dataset). New research directions are discussed in detail, including ways to improve the generalisation of machine learning methods, and move towards creating more stable presentation attack detection techniques that generalise across a wide range of unseen samples.

Keywords: Face Recognition, Presentation Attacks, Deep Learning, Generalisation

1. Introduction

The recent, significant improvements in biometric techniques have supplanted conventional authentication methods such as passwords, cards, and tokens over the past few decades [1]. These systems have facilitated more secure and automated authentication by utilising physical and behavioral traits. Face, fingerprint, iris, gait, handwritten signature, and voice are some of the traits utilized in biometrics [2]. The popularity of Face Recognition (FR) has increased significantly in recent times [3, 4]. The non-intrusive, user-friendly nature and low sensor cost account for the universality of FR [5]. Law enforcement, access control, surveillance systems, border security, and entertainment applications are typical applications [6, 7]. However, like any other authentication methods, vulnerabilities [8] affect FR systems. These ubiquitous systems are exposed to various attacks due to progressive technology. They include direct and indirect attacks [9]. Presentation attacks (PAs) [10], disguise [11], makeup [12], and plastic surgery [13] are different varieties of direct attacks. By showing a photo, or video of a live face, or wearing a facial mask, an imposter can be authenticated as a genuine user [14, 15]. This method of presenting fake facial attributes to FR systems is defined as presentation attacks and is commonly known as spoofing [5]. The tools such as photo, video, and mask, used by attackers, are called Presentation Attack Instruments (PAIs) [14].

Presentation attacks introduce various distortions and alterations to the sensor output images [16]. Compared to an authentic image, a spoof image may contain different noise content [17]. The spoofing image is prone to distortions like surface reflection, Moiré-effect, colour distortion, and shape deformation. This disparity between spoof and genuine images provides cues for the anti-spoofing methods to detect fake images [18]. Presentation Attack Detection (PAD) identifies whether the image is genuine or fake [10]. From Fig. 1, it is evident that PAs occur at the sensor. The sensor output is pre-processed for face detection and then PAD checks for spoofing in the image. If the presence of spoofing is confirmed, the system rejects access. If no attack is detected, the system processes the image for authentication and access is either granted or denied.

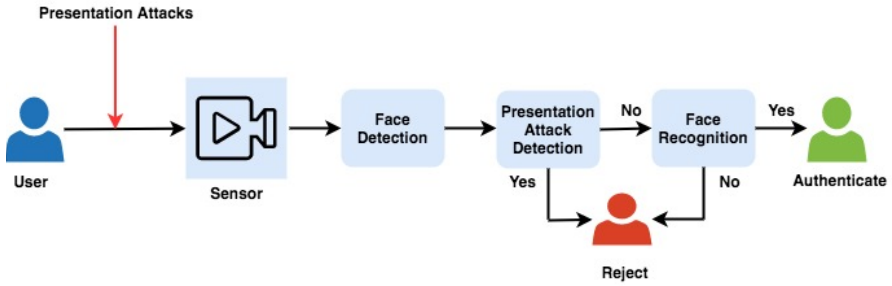


Figure 1: Face Recognition System with Presentation Attack Detection

PAD uses either sensor based methods or feature based methods [5]. Sensor-based methods (hardware methods) mainly involve additional hardware to identify PAs. In sensor based methods, the FR system will obtain more cues for PAD from additional auxiliary sensors [5]. Some examples for such additional sensors are Light Field Camera (LFC), multi-spectral sensors and 3D scanner. However, software associated with these systems facilitates feature extraction and spoof detection. In feature-based methods (software-based methods), the PAD involves processing features extracted from the captured face images [19, 20, 21]. Sensor-based methods relating to deep learning are covered in this paper but for a more complete overview the interested reader is referred to [22, 5]. Traditional feature-based methods adopted hand-crafted feature methods [23, 24] for PAD. Owing to the distinctive feature processing power, recently developed methods adopt deep learning for PAD [25]. Distinct methods were developed to detect PA as the result of considerable research that has been conducted on face PAD. These methods have performed impressively in a specific attack detection scenarios or with specific datasets, but were not necessarily capable of detecting unseen attacks.

Deep learning has brought progressive changes in PAD approaches. Unseen attack detection has been addressed using various deep learning methods in the last few years. Recently, this binary classification problem was even reformed as One Class Classification (OCC) problem. OCC techniques aimed to classify the genuine face accurately and consider all others as attacks. This approach assist to enhance generalisation and unseen attack detection. These OCC approaches include domain generalisation, anomaly detection, zero-shot and few shot learning. A number of extensive reviews on PAD already exist in the literature as in Table. 1. These investigations provided a thorough, in-depth technical review on presentation attacks and their detection methods. The authors discussed PAs and their variants. The reviews investigated generic taxonomy of PAD. However, recent deep learning approaches were less discussed in the existing literature. Hence, this review focuses primarily on recently proposed deep learning based face PAD.

Table 1: Reviews on face presentation attack detection

Author	Year	Attacks	CNN Methods	Generalisation	Discussion
Kähm and Damer [26]	2012	Photo	×	×	Generic taxonomy of anti-spoofing method based on different cues
Galbally et al. [27]	2014	Photo, Video, Mask	×	×	Generic taxonomy of anti-spoofing methods
Hadid [28]	2014	Photo, Video	×	✓	Fusion Methods, challenge Response methods, open issues including generalisation.
Ramachandra et al. [5]	2017	Photo, Video, 3D Mask	×	✓	Generic taxonomy of anti-spoofing methods, evaluation metrics, relevant international standardization.
Rakshit and Kisku [2]	2017	Photo, Video, 3D Mask, Plastic surgery	×	×	Generic taxonomy of anti-spoofing methods, generalisation.
Norzali et al. [29]	2017	Photo, Video, 3D Mask	×	×	Generic taxonomy of anti-spoofing methods, evaluation metrics.
Kumar et al. [19]	2017	Photo, Video, 3D Mask	×	×	Anti-spoofing methods
Mohammadi et al. [30]	2017	Photo, Video	✓	×	Vulnerabilities of deep learning based PAD
Souza et al. [14]	2018	Photo, Video, 3D Mask	×	×	Anti-spoofing methods, evaluation metrics.
Rattani et al. [21]	2018	Photo, Video, 3D Mask	×	×	Anti-spoofing in mobile devices
Hernandez-Ortega et al. [10]	2019	Photo, Video, 3D Mask, Plastic surgery, Make-up	×	×	Generic taxonomy of anti-spoofing method based on different cues
Raheem et al. [31]	2019	Photo, Video, 3D Mask	×	×	Generic taxonomy of anti-spoofing methods, evaluation metrics.
Wu et al. [32]	2019	Photo, Video, 3D Mask	✓	×	Recent trends in face anti-spoofing, face anti-spoofing used in industry.
Bhattacharjee et al. [33]	2019	Obfuscation Attacks	✓	✓	Various approaches in face anti-spoofing, evaluation metrics, one class classification
Kahilal and Kaur [34]	2019	Photo, Video, 3D Mask	×	×	Generic taxonomy of anti-spoofing methods
Munir and Khan [22]	2019	Photo, Video, 3D Mask	×	×	Multi-spectral aspects in face anti-spoofing
Jia et al. [35]	2020	3D Mask	✓	✓	A detailed investigation on various methods in 3D anti-spoofing.
Jia et al. [36]	2020	Not specified	✓	✓	Multiple aspects of mobile anti-spoofing including generalisation
Liu et al. [37]	2020	Not specified	×	×	Presents face anti-spoofing challenge and its outcomes

The main contributions of this review are:

- An extensive and detailed discussion, categorisation and evaluation of various types of attacks on face recognition, including 2D and 3D Face Presentation attacks.

- Systematic and in-depth technical discussion and evaluation of current face PAD and the state of the art methods including recent deep learning techniques. This review delves into the approaches used in face presentation attack detection. We present in detail recent trends in deep learning research (e.g. domain generalisation, anomaly detection and few-shot learning, domain adaptation and others) and how it has been applied to detect face presentation attacks.

- An extensive investigation of existing datasets based on the attack type, variants, modalities and size and detailed discussion of evaluation metrics used in face PAD context.

- A detailed evaluation of face presentation attacks detection limitations, which sheds light on some research gaps and challenges in this area and suggests future research directions to address these challenges

The article is organised as follows: Section. 2 presents attacks on face recognition systems and Section. 3 details a general taxonomy of presentation attack detection. Section. 4 includes thorough investigation of recent deep learning methods and techniques in the existing literature to enhance generalisation. Section. 5 and Section. 6 describe the face presentation attack detection datasets and evaluations metrics respectively. Section.7 highlights current open issues and introduces possible future directions, concluding the article.

2. Attacks on FR Systems

Attacks on FR system are generally classified into direct and indirect attacks. Direct attacks occur at the sensor stage by presenting forged facial artifacts. Indirect attacks affect matching, feature extraction, database and decision modules. The attacker should be aware of the system knowledge to execute these attacks [5]. Direct and indirect attacks influence the FR system as shown in the Fig. 2. Duplicating and introducing the facial artifacts to the FR system has become easier with technological improvements [27, 5]. Common direct attacks are:

- Presentation Attacks

- Disguised/makeup
- Modifications done through plastic surgery

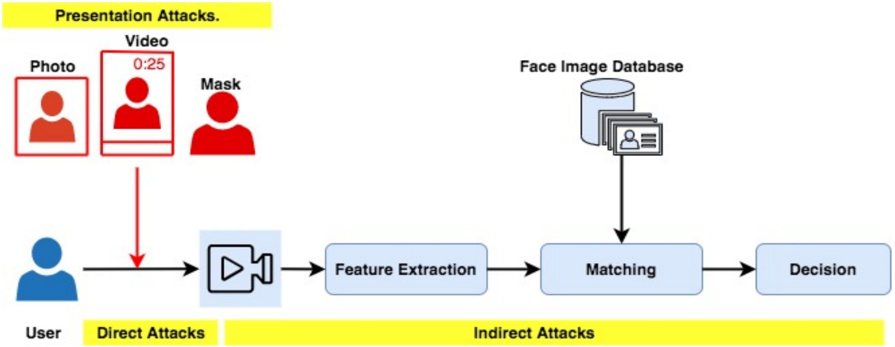


Figure 2: Attacks on Face Recognition system

Disguised faces are one type of direct attack. Disguise accessories can intentionally or unintentionally impersonate or obfuscate. Unintentional disguises include sunglasses, hats, or scarves. FR is vulnerable to various types of intentional and unintentional disguise accessories. The authors of [38] observed that the facial portions under disguise accessories provide false data and FR cannot use these for identifying a user. Hence disguise accessories facilitated the hiding or imitating of identity. These types of disguise attack are prominent in border crossing and airport security applications [11].

Makeup is another direct attack similar to disguised faces. It is harder to identify makeup attacks as they have close resemblance to the real face [39]. While keeping the genuine appearance of human face, makeup can easily obfuscate the true identity of the user. Among the direct attacks, it is easily available, cheaper and variant in nature.

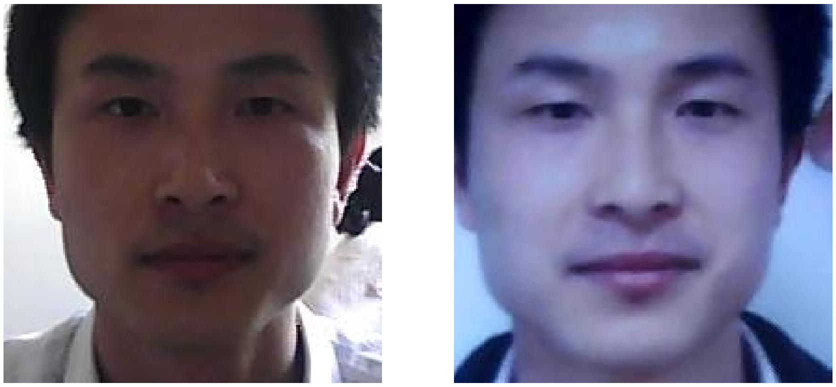
Plastic surgery is a direct attack, too. Face regions including nose, eyes, lips, ear, or bone structure are reformed to obtain desired appearances. These cause long-lasting changes in features in specific facial regions. The reference database may contain the pre-surgery sample for face recognition. In this case post surgery biometric recognition becomes challenging due to the alterations [40]. Some disease treatment surgeries can also unintentionally increase variations in facial appearance [2].

Attackers make use of eye glasses, facial hair and caps either to impersonate or obfuscate. Such effects are generated using adversarial methods too. These adversarial generated attacks are able to mislead the classifier in deep learning based FR systems [41]. These perturbations are physically imperceptible or even ignored by human eyes, yet capable of causing misclassification in FR systems [42]. Thus, synthetic images generated through adversarial methods and modified images with adversarial perturbation act as PAs [43]. Attackers add perturbations in two ways, ‘no target’ and ‘dodging’. In ‘no target’, the aim is to hide the identity of the user, whereas in ‘dodging’, perturbation is added to access the identity of a target user. The authors of [44] introduced an eye glass printing method to generate physically realisable attacks. Sharif et al. [45], using 3D printed eye glasses, generated attacks to execute impersonation. Using an infrared lighting cap [46] was able to create adversarial physical attacks. Adjusting the positions, size and intensity of the infrared dots generated by this cap, the attacker could pass through the security system. Nguyen et al. [47] proposed a more convenient method to create adversarial attacks using light projections. Real-time physical attacks were created changing camera-projector setting suitable to the attacking environment.

2.1. Presentation Attacks

Presentation attacks (PA) [48] are used either to impersonate or to obfuscate a user while passing through a FR system. Impersonation is carried out by copying a genuine user’s facial attributes to gain access through FRS. Obfuscation is used to hide the user’s identity using various methods such as glasses, makeup, disguised face and facial hair [49]. A generic FR system detects faces from the image or the video input and recognises authorised users with respect to the reference database. PAs have duplicate facial features in the form of photo, video or mask. This will assist the attacker to invade the security system if the FR does not have a detection module to differentiate between genuine and fake faces. Hence, PAs affect the proficiency of FR system in security applications [50].

PAs are broadly classified into 2D and 3D attacks as can be seen in Fig. 4. Photo attacks and replay attacks are 2D attacks [51], whereas mask attacks are included in 3D attacks [35].



(a) Bona-fide (b) Print Attack

Figure 3: Figure showing bonafide and print attack from NUAA Imposter database [52]

2D attacks are very common. They are carried out by presenting facial artifacts using photo or video to the sensor [5]. Flat printed photos, digital display of photos, eye-cut photos, warped photos are photo attack variants [14]. Fig. 3 gives an example of authentic and print attack images from NUAA Imposter database [52].

In cut-photo attacks there will be holes on the position of eyes and mouth. These help the imposter to imitate live features like eye blinking, mouth movements [14]. Spoofing of FR system which work based on the liveness of the user can be carried out using these types of photos. Such ways of spoofing are harder to detect compared to flat printed photo attacks [53].

Video attack is performed by presenting video of a genuine user to FR system [14, 5]. Using mobile, tablet or any other digital devices these videos are captured and displayed to the FR system in order to use them as PAIs [27, 10]. Since the video consists of both movement and background information, distinguishing fake user from bona fide user in these cases is a challenging problem [16].

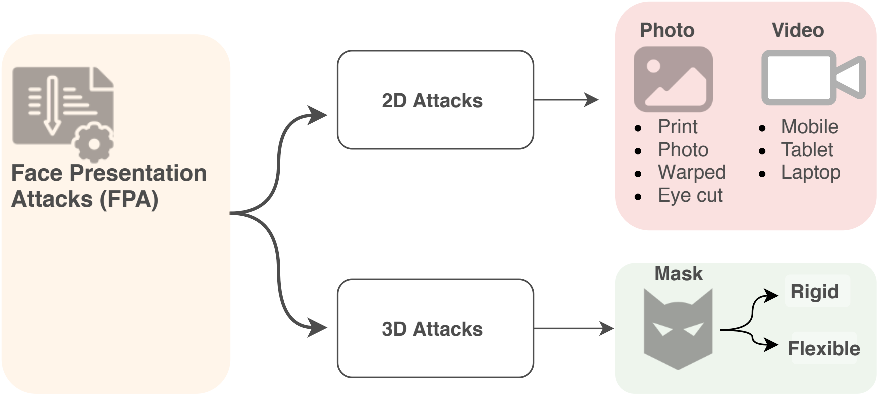


Figure 4: Types of Presentation Attacks

While FR sensors capture images for authentication, the imposter can wear a mask with features of a genuine user. 3D masks possess face-like depth and this is a challenge in detecting the 3D mask PA. Ramachandra et al. [54] experimented to find vulnerabilities in two commercial FR systems and observed that, due to the False Acceptance Rate (FAR) threshold, these systems were vulnerable to custom silicon mask. As the FAR threshold was set to lower values, the vulnerability decreased. In a similar study, Bhattacharjee et al. [55] investigated custom made silicon masks and found that FR systems were highly vulnerable to flexible mask attacks.

There are various types of masks made of distinct materials. Much of the literature covers 2D type attacks as, historically, it was difficult and costlier to produce 3D masks. Lately there have been developments in 3D printing technologies which have provided cheaper and easier ways to produce 3D masks [35]. 3D masks are made of different materials [40]. Hard/rigid mask can be made from paper, resin or plastic. These masks are used as an improved variant of photo attacks. These cheaper types of mask appear visually very similar to real faces due the enhanced printing options available nowadays. Masks which are produced using silicon or latex are soft, flexible and adapt to different facial shapes and sizes. They have close similarity with genuine facial texture and colour. It makes these soft masks more challenging to detect than rigid masks.

3. Presentation Attack Detection

In feature-based PAD methods, spoof detection involves processing features extracted from the captured face images [19, 20, 48]. Texture, temporal data, image quality and life signs are typical features processed to identify PA. Feature based methods are classified as two types: static and dynamic [5]. Texture and image quality based PAD methods are examples of static approaches, whereas temporal (or motion-based) and vital signals based methods are dynamic approaches.

Static approaches include texture and image quality based techniques. They do not rely on temporal information and a single image is processed at a time to detect spoofing [10, 2]. By processing each frame independently, static approaches can perform anti-spoofing tasks using video. The processed outcome of the majority of frames are taken into account to form the final decision. Due to their performance, low computation and low cost, static approaches are popular. In comparison with dynamic approaches, static approaches are faster [5].

Through micro-textural analysis of the facial image, textural PAD methods distinguish real images from fake ones [10]. These methods identify photo and replay attacks [5]. Local Binary Pattern (LBP) descriptors are the most widely used technique in texture based-PAD methods. Authors of [23] proposed a PAD method using LBP for textural analysis for photo attacks. Replay attack detection was explored in [24] using the same technique tuned for video attacks. The advantages of these methods were easy deployment and no user interaction. However, these methods required feature vectors and exhibited poor performance with low resolution images [56].

Presentation attacks affect the quality of the image [10]. Spoofing images are prone to distortions like surface reflection, Moiré-effect, colour distortion, and shape deformation [18]. In [16], the authors detailed the various distortions an image may be subject to due to spoofing medium, camera and printing. Spoofing medium (LCD or paper) causes specular reflection. Blur is introduced if the camera is out of focus while capturing the spoofing image. Reduced resolution of printed paper or LCD can also create colour distortion. Spoofing mediums add noise to the image [17]. The frequency histogram a spoof image would be different to that of a genuine image. Face PAD systems use these quality variations in the image as cues while performing spoof detection.

Dynamic approaches depend upon temporal information to identify the presence of spoofing in FR systems [57]. They process life signs or motion to verify the liveness in the input presented to the facial sensor in FR system. In dynamic approaches, performing temporal feature analysis, based on relative motion in the video provides information for spoof detection. Hence, dynamic approaches require more computational time compared to static approaches [5]. Some dynamic approaches rely on life signs too. Pulse, eye blinking, lip movement, head rotation can be used to confirm the liveness in FR system [10].

A temporal information based algorithm Dynamic Mode Decomposition (DMD) was used in [58] to identify liveness. The authors used eye blinking and lip movements as motion cues. Motion based PAD techniques demand user co-operation during the identifying process. This affects the processing time in FR system [10]. Some motion based methods exploit impulsive movements of the facial parts in the input videos [59]. In [60], the authors followed a multiple-motion-cue-based method, considering eye-blinking, chin and lip movement. The authors of [61] presented liveness detection methods based on pupil tracking. Remote Photo Plethysmography (rPPG) is used for acquisition of vital signals such as pulse or heart rate without contact with the human body. Since these vital signals are extracted from live faces, they acts as the perfect cues for liveness. Face liveness detection methods presented by authors of [62] utilized pulse cues from videos. Pulse detection using rPPG was effective in 3D mask attack detection [63]. In [64], the authors presented a face liveness detection approach based on blood flow analysis. rPPG and patch CNN based method was adopted in [65] to detect face liveness too.

Face recognition systems process static and dynamic cues using different techniques for spoof detection. Earlier feature-based methods mainly deployed hand-crafted features in detecting presentation attacks. Local Binary Patterns (LBP) [24, 23], Histogram of Oriented Gradient descriptors (HOG) [66, 67], Speeded-Up Robust Features (SURF) [68], Difference of Gaussian (DoG) [69, 52] were the techniques adopted in hand-crafted feature methods. The hand-crafted feature methods commonly used texture analysis. Textural features vary with the variation in spoofing medium and devices. This leads to poor generalisation in these methods [70]. The emergence of deep learning methods provided effective feature learning in many applications. Moreover, deep learning methods provided better detection performance compared to hand-crafted methods. Thus the most recent trends demonstrate a large shift towards deep learning based approaches in face PAD.

4. Recent trends in deep learning based PAD

Deep learning-based methods have been successfully applied to various domains including speech enhancement and recognition [71], lip reading from visual content [72], analysing intractable and complex biological datasets [73], security and intrusion detection [74], and others. Convolutional neural networks in particular, have introduced remarkable developments in computer vision applications, especially in biometrics [75]. Deep learning, along with its inherent feature learning capability, constructed a novel path to solve the anti-spoofing challenge. Existing methods based on deep neural networks, show excellent intra-dataset performance. However, these methods have also exhibited poor cross-dataset performance and unseen attack detection [76, 77].

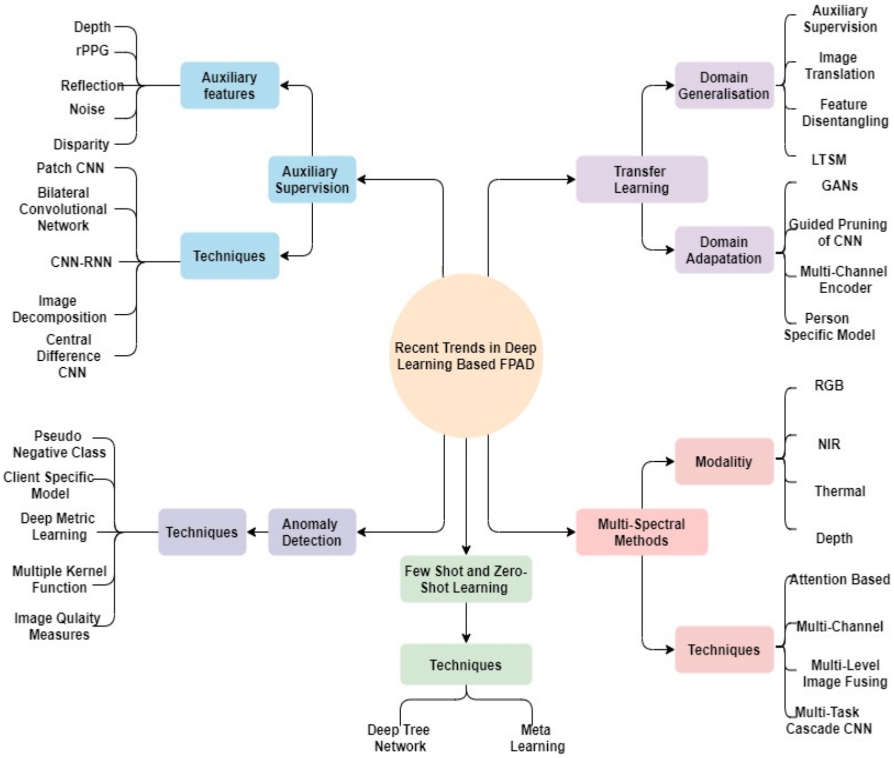


Figure 5: Recent trends in deep learning based FPAD

In the last few years, there has been a trend towards improving generalisation in PAD. In particular, unseen attack detection methods involve trying to accurately classify genuine samples and consider any sample except genuine ones as attacks. Some existing approaches have used only genuine samples for training so that the proper clustering and classification of genuine face would lead to desired detection of unseen attacks. These methods followed one class classification, as opposed to earlier models which followed binary classification for face PAD. A typology of recent trends in deep learning based FPAD is shown in Figure. 5.

4.1. Transfer Learning

Transfer learning is the process of re-utilising the learned features from a base network using base dataset to a target network to be trained with target dataset and task. Transfer learning helps to avoid overfitting when the training data is limited [78]. As training is not started from scratch, it also saves on computational resources. Nagpal et al. [79] analysed different CNN models for face anti-spoofing and their performance in detecting presentation attacks. Based on their research the authors recommended transfer learning with a deeper model utilizing lower learning rates for restricted computational resources. Lucena et al. implemented transfer learning for spoof detection in their work [80]. Among the deep learning methods deployed in FPAD, transfer learning is the most common one.

Domain adaptation and domain generalisation utilised a transfer learning approach to improve generalisation in FPAD. In domain adaptation, information from a source domain is transferred to a target domain using different techniques [81, 82]. Yu et al. [83] developed a neural architecture search based face anti-spoofing (NAS-FAS) system. This method used central difference convolution and pooling. Transfer learning approach was applied on NAS for spoof detection task. However, a cross-dataset evaluation for 3D mask attacks with NAS-FAS showed that challenges still remain the the generalisation capacity of even transfer learning approaches.

4.1.1. Domain adaptation

Domain adaptation mitigates the disparity between source and target domains. It facilitates feature learning in scenarios with limited training data. Hence, generalisation capacity of face PAD can be improved using this method. In domain adaptation the model learns from the source domain on related distinct target domain [84]. Hence, recent research has utilised this technique to mitigate domain shift. Yang et al. [81] introduced domain adaptation in their research on personal specific face anti-spoofing approach.

This approach transferred source domain subject specific information on real and fake samples. This information facilitated synthesis of virtual fake samples for subjects without fake samples in target domain. Spoof detection was performed using a trained classifier for each person in this method. In real life scenarios, there would be genuine samples without corresponding fake samples. However, personal specific models required samples from all attack variants in target domain to attain desired performance. This method also demanded more source domain fake samples for generalisation enhancement.

Inspired by the applications of Generative Adversarial Networks (GANs) [85] in various compute vision applications, Wang et al. [84] presented a domain adaptation method using them to address FPAD problem. Adversarial domain adaptation combined with deep metric learning assisted this model to outperform other state of the art methods in both cross-dataset and intra-dataset evaluation. The authors extended this method using an unsupervised adversarial domain adaptation technique (UDA-Net) in [86]. UDA-Net carried out unsupervised adversarial domain adaptation. This facilitated extraction of common features associated with both target and source domains. As DR-Net assisted to transfer domain independent information, it enabled better spoof detection in a unlabeled target domain. The authors carried out extensive evaluation on more publicly available datasets.

Zhou et al. [87] adopted a multi layer domain adaptation technique for spoof detection in face recognition systems. In order to reduce the disparity between source and target domains, the authors used a Multi Layer Maximum Mean Discrepancy (ML-MMD). Similarly, Nikisins et al. [82] used domain adaptation by transferring facial features from RGB domain to multispectral domain. Domain adaptation was carried out using autoencoders. In this model, a set of multi-channel encoders were used for feature extraction. Classification of these features were performed by Multi Layer Perceptron (MLP). The authors of [88] evaluated domain adaptation through domain guided pruning of CNN. Recent domain adaptation research in face PAD are presented in Table. 2.

Table 2: Face PAD using domain adaptation method

Author	**Method**	**year**	**Datasets**
Yang et al. [81]	Person Specific Anti-spoofing	2015	CASIA, REPLAY ATTACK
Wang et al. [84]	Adversarial Domain Adaptation	2019	CASIA, MSU-MFSD, REPLAY ATTACK
Zhou et al. [87]	Multi Layer Maximum Mean Discrepancy	2019	CASIA, REPLAY ATTACK
Nikisins et al. [82]	Multi-Channel Encoder	2019	WMCA
Mohammadi et al. [88]	Domain guided pruning of CNN	2020	REPLAY Mobile, SWAN, WMCA
Wang et al. [86]	Unsupervised Adversarial Domain Adaptation	2020	Idiap, MSU, CASIA, ROSE-YOUTU, CASIA-SURF, OULU

In domain adaptation, trained features are aligned to the target features to achieve better generalisation capacity through adapting the features of the target or test domain. However, for unseen attacks cases, the target domain may be unknown and this would impact domain adaption.

4.1.2. Domain Generalisation

Domain generalisation is one of the techniques adopted by the biometric community to acquire generalisation in unseen attack scenarios. In existing face PAD methods, there is bias towards the cues learned from training data. This impedes generalisation against unseen attacks with different environments, devices, lighting conditions or materials.

Costa-Pazo et al. [89] adopted domain generalisation for PAD. The authors designed a framework Generalised PAD (GPAD) to address the generalisation problem and suggested an aggregate dataset with variance in attacks, lighting, capture devices, and resolution. The GRAD-GPAD (Generalisation Representation over Aggregated Datasets for generalised Presentation Attack Detection) provided a common evaluation method for face anti-spoofing techniques.

Saha et al. [90] addressed domain shift in face PAD using a domain agnostic model. A class-conditional domain discriminator and gradient reversal layer were utilised to learn domain independent features. Source domain features were learned through training using multiple datasets. The model showed improved generalised feature learning across multiple domains for print and video attacks. The multiple domains were formed due to the variations in illumination, background, printers, display screens, and the quality of recording devices. Wang et al. [91] utilised GANs to address unseen attack detection. The adversarial domain adaptation facilitated transferring source domain features to target domain. This technique included a Disentangled Representation learning (DR-net) and Multi Domain learning (MD-net). DR-net learned disentangled features. MD-net learned the generalised features across multiple domains using these disentangled features from these domains. Evaluation with CASIA, REPLAY -ATTACK, MSU and OULU-NPU datasets provided an improved cross-domain performance compared to existing state of the art methods. However, the experiments also confirmed the fact that a larger dataset with more attack variants would be required for effective unseen attack detection.

Shao et al. [92] proposed another domain generalisation method without using the target domain data. Adaptive and automatic learning of generalised features was facilitated by a multi adversarial deep domain generalisation module. Integrating a dual-force triplet-mining constraint enhanced the disparity in the generalised feature space. The model used auxiliary depth supervision to further improve generalisation. Unlike the aforementioned models, Jia et al. [93] followed a single domain generalisation. Retaining the boundary of feature domains of real and fake faces has become increasingly difficult due to novel attacks. In order to avoid grouping and extracting generalised features from multiple domains, the authors used a single domain. Use of Asymmetric Triplet Mining ensured effective clustering of real face features while spreading away the fake ones. Zhang et al. [94] introduced a FPAD model disentangling features into live and content features. Depth supervision and translated images were utilised in this model.

Existing domain generalisation approach transferred generalised features from source domain to a pre-defined distribution. However, this distribution might not be an optimal feature space [92]. Learning discriminant features requires multiple components in these models. Elimination of any of these feature discriminators might deteriorate the generalisation capability of the model [93].

4.2. Anomaly Detection

Unseen attack detection was addressed using anomaly detection approach in recent research. Anomaly detection followed one class classification. From Table. 3, it is evident that this approach had gained more popularity in last few years for unseen attack detection. In face PAD problem genuine or live face images are considered normal samples, whereas all possible attacks forms the anomalous sample space. It has been found that the genuine class has lower variance within the feature distribution and a forms a close cluster. They had more generalised features than the attacks. Attacks, on the other hand, can vary substantially from one another. The higher variance in attacks results in anomalies in the feature space. Using this close cluster behaviour of genuine samples in the feature space, anomaly detection techniques have classified authentic faces more accurately. Any samples outside the margin of the genuine sample cluster would be considered as the attacks. Since the real face sample has a defined class, unseen attacks can be detected.

Arashloo et al. [95] introduced anomaly detection for face PAD. This technique used only genuine face samples for training. The authors set up a new evaluation protocol to gauge the affects of unseen attacks. In terms of generalisation, these fake or negative samples represented all the spoofing samples. This method produced comparable results with the models using binary classification. In [96], Arashloo and Kittler proposed a similar technique to address unseen attack scenarios. The authors incorporated multiple kernel fusion, client-specific modelling, sparse regularisation and probabilistic modelling of score distributions to enhance the performance of the system. Through extensive evaluation using different datasets, it was shown that the method performed better than the existing state of the art models in unseen attack detection.

Anomaly detection was explored by Nikisins et al. [97] too. Similar to [95], the authors used only genuine samples for training. Feature space was created using Image Quality Measures (IMQ) in this model. A Gaussian Mixture Model (GMM) to find out the probability distribution of genuine samples. Combining REPLAY-ATTACK, Replay-Mobile and MSU-MFSD public datasets, an aggregate dataset was formed. Compared to the binary classification methods, the designed model exhibited better generalisation when tested with the aggregate dataset. In a similar research, Fatemifar et al [98] used a client specific model. In one class classification, each biometric trait has scores which would be distinct for genuine and attack samples. In this way, a threshold can be defined to distinguish between real and fake images. A client specific threshold was set which provided better distinctive capability to categorise genuine and attacks. This method exploited only real face information to implement a perfect anomaly detection approach. However, more mechanisms might be needed to refine single class learners if the training data included fake samples. Fatemifar et al. [99] presented another subject specific model. They fused the individual one class classifier using a new normalisation technique in this ensemble learning method. A weighted average fusion strategy was used in the model.

Table 3: Anomaly detection approaches in recent face PAD research

Author	**Year**	**Remarks**
Arashloo et al. [95]	2017	A new evaluation protocol to detect the affects of unseen attacks
Arashloo and Kittler [96]	2018	Multiple kernel fusion, client-specific modelling, sparse regularisation, probabilistic modelling of score distributions
Nikisins et al. [97]	2018	Image Quality Measures (IQM), Gaussian Mixture Model (GMM)
Fatemifar et al. [98]	2019	Subject specific models
P ´erez-Cabo et al. [100]	2019	Deep Metric Learning
Fatemifar et al. [99]	2019	Client Specific Modeling
Abduh & Ivrissimtzis [101]	2020	Convolutional Autoencoder, in-the-wild training images
Li et al. [102]	2020	Hypersphere loss function
Feng et al. [103]	2020	A spoof cue generator and an auxiliary classifier.
Baweja et al. [104]	2020	Pseudo-negative class samples

Deep metric learning was used in anomaly detection to address generalisation. Perez-Cabo et al. [100] proposed this method and evaluation was carried out using GRAD-GPAD [89]. Metric learning based loss provided lower intra-class variance and higher inter-class separability. Better classification of fake and genuine samples resulted using metric learning based approach. Feng et al. [103], presented another anomaly detection based face PAD. In this method, the framework had a spoof cue generator and an auxiliary classifier. The model used a residual learning network to extract the spoof cues. The method achieved good state of the art performance in unseen attack detection. In [102], Li et al. addressed face PAD in an open setting with an anomaly detection method. They introduced a new hypersphere loss function for end-to-end learning. Real faces formed a close cluster near to the origin of the hypersphere sustaining intra-class compactness. The attack samples scattered at a specific distance from the genuine face cluster in the feature space to maintain the predefined margin between real and fake features. Hypersphere loss identified these attacks directly without using a separate classifier. Baweja et al. [104] introduced a novel training approach for anomaly detection. The absence of negative samples made end-to-end learning in one class classification non-viable. Hence, the authors proposed a ”Pseudo-negative class” sample feature space, which helped the model in learning better decision boundaries between genuine and fake samples. The pseudo-negative class was modeled using a Gaussian distribution. Unlike other existing OCC models, end-to-end learning was carried out for both classifier and feature representation. The authors of [101] included in-the-wild images in the training dataset of a one class classifier. These images were recorded in an uncontrolled environment. Hence, features learned during training facilitated model operation in uncontrolled environment. This enhanced unseen attack detection.

4.3. Few-shot and zero-shot learning

Few-shot learning (FSL) [105] is the process of learning from few samples with the supervised data. FSL is suitable to applications which require large scale data from supervision. FSL has only a small number of labelled target samples. When the number of these samples for target class is zero, FSL is called zero-shot learning. Since the requirement of target samples are very few or zero (in zero-shot scenario), FSL is suitable for detecting unseen or novel attacks. Recent research made use of this advantage of FSL to detect unseen attacks in face PAD.

Qin et al. [106] proposed face PAD using zero-shot and few-shot approaches. The authors designed Adaptive Inner-update Meta Face Anti-

Spoofing (AIM-FAS) with meta learning. Using pre-defined live and fake samples along with a few samples of unknown attacks, the model carried out spoof detection. The meta learner provided better discrimination between live faces and attacks. With adaptive inner update, the discriminative capacity enhanced, improving generalisation. Liu et al. [107] used a zero-shot approach to address the unseen attack detection in face PAD. The authors used a deep tree network to learn the semantic attributes of pre-defined attacks in unsupervised methods. Even though live samples clustered well in the feature space, they positioned very close to a specific group of attacks like transparent mask, funny face, obfuscation makeup and paper glasses. This made detection more challenging in such scenarios, and implies that these attacks might be more challenging to detect.

4.4. Auxiliary Methods

Anti-spoofing is considered as a binary classification problem. Hence, the majority of the anti-spoofing models follow binary supervision. Nevertheless, binary supervision has demerits too. Even though it provides arbitrary cues to detect spoofing, some of the spoof patterns may disappear over the feature duplication process. This results in poor generalisation [108]. To overcome poor generalisation, auxiliary supervision has been used in a number of recent researches. It has been shown that auxiliary supervision with end-to-end learning can provide better anti-spoofing [109]. The methods which use auxiliary data are presented in the Table. 4. As in the table, depth was used as an auxiliary feature in the majority of the existing models.

Table 4: PAD with auxiliary supervision

Method	**Auxiliary Cues**	**Attacks**
Patch CNN [109]	Depth	Print, Replay
CNN-RNN [108]	Depth, rPPG	Print, Replay
Frame-level CNN [110]	Pixel wise binary	Print, Replay
CNN with OFFB and ConvGR [111]	Depth	Print, Replay
Central Difference CNN [112]	Depth	Print, Replay
Multi-Spectral Central Difference CNN [113]	Pixel wise	Print
Bilateral Convolutional Network(BCN) [114]	Human material	Print,Replay
Bipartite Auxiliary Supervised Network (BASN) [115]	Bipartite (Depth, Reflection)	Print, Replay
Contextual Patch-Based CNN [65]	rPPG	2D, 3D
Patch CNN [116]	Depth	Print, Video
SLNet [117]	Disparity	Print, Video
Image Decomposition [17]	Noise	Photo

Atoum et al. [109] introduced the depth supervision for anti-spoofing by proposing a depth supervised patch based CNN. From the random patches, local features are extracted. These features were fused with a depth map to identify spoofing. A similar auxiliary supervised approach using depth and Remote Photoplethysmography (rPPG) supervision was proposed by Liu et al. [108]. The authors used a CNN and recurrent neural network (RNN) combination for spoof detection. rPPG facilitated temporal information extraction using the difference in live signals for live face and spoof image. Distinct from the above-mentioned single frame PAD methods with auxiliary supervision [109, 108], a multi-frame approach was followed by Wang et al. in [111]. This approach exploited temporal information along with depth supervision. The authors followed the distinguishing patterns of temporal depth and motion between live and spoof images in the temporal domain. This approach facilitated efficient spoof detection under depth supervision by examining complex facial variations and motions.

Auxiliary methods used depth and temporal features for supervision. The acquisition and processing of these features might take longer time. Nevertheless, in real-time scenario, especially in mobile devices this delay would not be acceptable. As the depth calculation consumed more computational resources and time, George et al. [110] followed a pixel wise supervision PAD method. This method was claimed as a suitable approach for mobile devices as it avoided the pixel wise depth calculation. In order to extract more generalisable features in auxiliary supervised PAD, Kim et al. introduced a novel Bipartite Auxiliary Supervised Network (BASN) [115]. This approach used auxiliary cues from both live face and spoof images, distinct from existing PAD methods with auxiliary supervision.

Following the aforementioned auxiliary supervised methods and leveraging the Central Difference Convolution (CDC), Yu et al. [112] introduced a spoof detection approach using Central Difference Convolutional Network (CDCN). By utilising Neural Architecture Search (NAS) architecture, low, mid and high level features were extracted. These features were fused using a Multi-scale Attention Fusion Module (MAFM). CDC provided better results by combining intensity and gradient information. Apart from achieving generalisation in face pose, expression, spoof medium, cross/unknown attack variants, this approach showed considerable performance in terms of domain shift. The authors extended the methods incorporating multi-spectral mode in [113] using two fusion strategies for the modalities. The fusion was done either by input-level fusion via concatenating three-modal inputs to $256x256x9$ directly or score-level fusion via weighting the predicted score from each modality. Yu et al. [114] also proposed a human material recognition model for face spoof detection. The authors included a Bilateral

Convolutional Network (BCN) for capturing human material patterns. The BCN was able to learn macro-micro features associated with material. A multi-level feature refinement module along with multi-headed supervision facilitated enhanced BCN performance by refining multi-scale features and learning shared features.

Authors of [65] proposed a method incorporating rPPG and textural information to attain generalisation in terms of 2D and 3D mask attacks. Multi-scale long term statistical spectral features for rPPG information was incorporated with contextual patch CNN. Remote Photoplethysmography (rPPG) provided 3D mask and photo attack detection while textural cues identified the replay attacks. Liu et al. [116] developed a face PAD combining Patch CNN and Depth based CNN. This approach was designed as a PAD for mobile devices. Depth based CNN showed degraded performance for low resolution images, whereas Patch based CNN showed low performance for high resolution images. The combination of these two improved the overall PAD performance in mobile devices. Unseen attack detection was addressed by learning disparity maps and training end-to-end classifier simultaneously. Rehman et al. [117] proposed an approach similar to the depth supervised auxiliary method. The learned disparity maps facilitated better detection of unseen attacks. Auxiliary supervision was investigated by Jourabloo et al. [17], too. They set up the auxiliary supervision of CNN to obtain the noise pattern and showed how different spoof mediums exhibited different noise patterns. In particular, noise patterns of live and fake image were different. End-to-end training of a CNN distinguished accurately between live and spoof accurately. Authors of [118] proposed a novel model, Spatio-Temporal Anti-Spoofing Network (STASN) to differentiate between live and spoofed faces. For anti-spoofing both temporal and spatial cues were used. The model used a new data synthesis method which provided a huge amount of training data. STASN combined with extensive training data provided improved performance when compared with the state of the art methods.

4.5. Multi-spectral methods

In a FRS, PAs occur in the visible light range. However, more cues on attacks are available from a other spectral images [22]. Multi spectral face PAD approaches in recent literature are listed in Table. 5.

Jiang et al. [119] proposed a multi-spectral presentation attack detection approach to detect 3D mask and print attacks based on visible spectrum (VIS) and near infra red (NIR) images. Similarly George et al. [120] used multi-channels (VIS, NIR and Thermal) and transfer learning to enhance performance. The method failed in identifying scenarios like prescribed glasses and facial hair attacks. Enhanced performance provided by extended-range imaging was utilized to detect PAIs in [121].

Kotwal et al. [121] addressed custom silicone mask based impersonation PAD by deploying multi channel inputs and CNN. Extracted feature vectors from CNN were classified using a logistic regression classifier. A two stream convolutional neural network approach was set up in [122]. Two imaging spaces, RGB and Multi-Scale Retinex (MSR) were used in this approach to extract textural features and high-frequency information. The model was found to be insusceptible to illumination changes. A multi-spectral method to identify disguise was described by Dhamecha et al [38]. This method classified facial portions into patches of biometric and non-biometric based on the presence of disguise tools and then performed a recognition task.

Table 5: Multi spectral anti-spoofing methods

Method	**Modality**	**Attacks**	**Databases**
Multi Level Image Fusing [119]	RGB, NIR	Print, 3D	CGIT PMT
Multi Channel CNN [120]	RGB, NIR, Thermal, Depth	2D, 3D	WMCA
Attention based Two Stream CNN[122]	RGB, MSR	Print, Replay	CASIA FASD, REPAY ATTACK, OULU
Multi Spectral Disguise Detection [38]	RGB, Thermal	Disguise	BVSD, IHTD
Multi Spectral Deep Embedding[121]	RGB, NIR, Thermal	Silicon Mask	XCSMAD
NIR Silent Liveness Detection Network Architecture [123]	NIR	Photo	Proprietary Dataset
Multi-modal FPAD with Spatial and Channel Attention [124]	RGB,IR,Depth	Photo	CASIA-SURF
Multiple Categories Image Translation GAN [125]	RGB, NIR	Photo, Video	CASIA-MFSD, REPLAY-ATTACK, Proprietary Dataset
Multi-Task cascaded CNN [126]	RGB, IR	Photo, Video	CASIA-MFSD, REPLAY-ATTACK, NenuLD

Fan et al. proposed and evaluated NIR and VIS methods with NIR and VIS datasets respectively [123]. Through the experiments conducted, the authors verified the capability of NIR methods compared to VIS method. As per their observation, NIR provided more distinct features and NIR camera itself has some resistance to spoofing as it could not take images of replay attack using mobile and high colour photos. Jiang et al. [125] utilised the cues from visible spectrum (VIS) and Near Infra Red (NIR) images. In this work, NIR images were synthesised using GANs [127] through image translation technique. The VIS and NIR pair gave cues for better spoof detection. Image translation using GAN provided required NIR image.

Liu et al. [126] proposed a PAD approach using IR and RGB images. The authors used a Multi-Task cascaded CNN (MTCNN). This approach exhibited lower responding time, making it suitable for real world applications. Wang et al. [124] presented another multi-modal technique to detect spoofed faces. Using RGB, IR and depth modalities, the authors used an attention mechanism to capture information to detect spoofing. These three modalities and their combination trained a ResNet-18 model and were classified using the combination of softmax loss and center loss.

Authors of [82] used domain adaptation to transfer source domain information from VIS domain to multi-spectral target domain. These multi-spectral methods were able to enhance spoof detection using reflection invariant cues obtained through extended imagery. However, these methods required an additional sensor along with VIS camera. Similar to existing other CNN based PAD methods, multi-spectral methods also required larger dataset with more attack variants in all modalities.

5. Datasets

Datasets have pivotal role in the performance of any presentation attack detection method. Generalisation of PAD relies on variance in samples of a dataset. Access to a wider variety of PAs facilitates the learning of more attack features during the training process. This eventually leads the system to detect the PAs of wide range. Samples of print attack images with different illumination conditions are shown in Figure. 6. Other attack variants include replay attacks, 3D mask attacks and its variants.

It is evident from Table. 6 that existing datasets consist of more 2D attacks than 3D attacks [128, 5]. However, diverse novel attacks are increasing with progressive technology. Dataset diversity is decided by PAs and their variants. Factors such as environment, recording set up, illumination, pose, expression and spoofing medium also affect the dataset content.

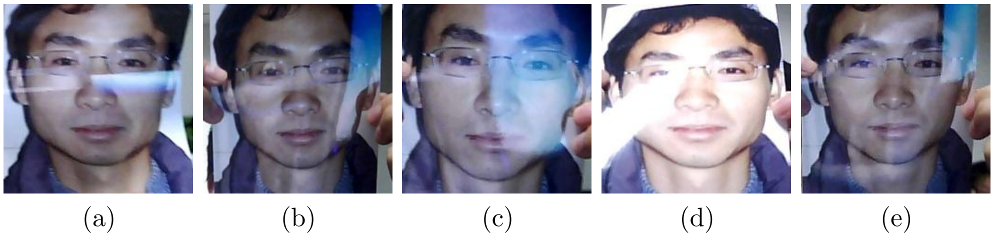


Figure 6: Print attack images from NUAA Imposter Dataset [52]

Table 6: Face spoof datasets

Dataset	**Year**	**Subjects**	**Samples**	**Modality**	**Attacks**
NUAA [52]	2010	15	12,641	RGB	Print
CASIA-MFSD [129]	2012	50	600	RGB	Print, Replay
Replay-Attack [24]	2012	50	1,200	RGB	Print, Replay
YMU [130]	2012	151	604	RGB	Makeup
ERPA [131]	2013	5	86	RGB, Depth, IR, Thermal	3D Silicon/resin Mask
MIW [132]	2013	125	154	RGB	Makeup
MLFP [133]	2013	10	1,350	RGB, Thermal	3D Latex, Paper Mask
GUC-LiFFAD [134]	2015	80	4,826	RGB	Print, Replay
MSU-MFSD [16]	2015	35	440	RGB	Print, Replay
3DFS-DB [135]	2016	26	520	RGB, IR	2D/3D Mask
3DMAD [136]	2016	17	255	RGB, Depth	3D Mask
HKBU MARs [137]	2016	12	1,008	RGB	3D Rigid Mask
MSSPOOF [6]	2016	21	4,704	RGB, IR	Print
Replay-Mobile [138]	2016	40	1,030	RGB	Print, Replay
BRSU [139]	2017	50	141	RGB, IR	3D Masks, Facial disguise
CIGIT-PPM [119]	2017	72	93,358	RGB, IR	Print, 3D Mask
EMSPAD [140]	2017	50	14,000	7-band multi-spectral data	Print
MIFS [141]	2017	107	416	RGB	Makeup
Oulu-NPU [142]	2017	55	5940	RGB	Print, Replay
SMAD [143]	2017	From internet	130	RGB	3D Silicon Mask
CS- MAD [55]	2018	14	308	RGB, IR, Depth, LWIR	3D Silicon Mask
DFW [144]	2018	1000	11,155	RGB	Disguise
Rose-Youtu [145]	2018	20	3350	RGB	2D, 3D
SiW [108]	2018	165	4620	RGB	Print, Replay
WMCA [51]	2018	72	6716	RGB, Dept, IR, Thermal	Print, Replay, 2D/3D Mask
3DMA [146]	2019	115	920	RGB, IR	3D Mask
AIM [147]	2019	72	456	RGB	Makeup
CASIA-SURF [148]	2019	1000	21000	RGB, Depth, IR	Print, Cut
I^{2}BVSD [38]	2019	75	681	RGB, Thermal	3D Facial Disguise
LCC FASD [149]	2019	243	18827	RGB	Photo
PR-FSAD [150]	2019	30	127440	RGB	Print, Replay
SiW-M [107]	2019	493	1,630	RGB	Print, Replay, 3D Mask, Makeup
WFFD [151]	2019	745	2300	RGB	Wax figures
CASIA SURF CeFA [152]	2020	1,607	23538	RGB, Depth, IR	2D, 3D
CelebA-Spoof [153]	2020	10177	625537	RGB	Print, Replay, 3D, Paper cut

Jiang et al. [119] introduced a dataset, “CIGIT Paired VIS and NIR images for Photo and Mask attacks” (CIGIT-PPM) incorporating RGB images and 3D attacks. The dataset shows variance in terms of attacks, medium of spoofing, recording environment, pose, expression, glasses/no glasses, resolution and distance. George et al. [120] created a multi modal dataset, Wide Multi-Channel presentation Attack (WMCA). 2D and 3D attacks were included in this dataset. The dataset comprises various imaging sensors, attacks, illumination and recording environments. Multi-modal images provided features which assisted in better PA detection. Datasets with different modalities are shown in Table. 7.

Table 7: Multi-spectral datasets

Database	**Year**	**Modality**	**Samples**	**Attacks**
ERPA [131]	2013	RGB, Depth, IR, Thermal	86	3D Silicon/ resin Mask
MLFP [133]	2013	RGB, Thermal	1350	3D Latex/ Paper Mask
I^{2}BVSD [154]	2014	RGB, Thermal	681	3D Facial Disguise
3DMAD [136]	2016	RGB, Depth	255	3D Mask
MSSPOOF [6]	2016	RGB, NIR	4704	Print
EMSPAD [140]	2017	7-band multi-spectral data	14,000	Print
BRSU [139]	2017	RGB, 4 SWIR bands	-	3D Masks, Facial disguise
CIGIT-PPM [119]	2017	RGB, NIR	93358	Print, 3D Mask
WMCA [51]	2018	RGB, Depth, IR, Thermal	6716	Print, Replay, 2D/ 3D Mask
3DMA [146]	2019	RGB, NIR	920	3D Mask
CASIA-SURF [148]	2019	RGB, Depth, IR	21000	Print, Eye-Cut photo
CASIA-SURF CeFA [152]	2020	RGB, Depth, IR	23538	2D, 3D

Dhamecha et al. [38] developed a multi-spectral dataset for disguise attacks called IIITD: In and Beyond Visible Spectrum Disguise (I^{2}BVSD). This dataset consists of 75 subjects with various disguise accessories. Both visible and thermal spectra were considered for data acquisition. The authors introduced distinct disguise variants for dataset as:

- Without disguise
- Variations in hair styles
- Variations due to beard and mustache
- Variations due to glasses
- Variations due to cap and hat
- Variations due to mask
- Multiple variations

Disguised Faces in the Wild (DFW) dataset [155] is a similar dataset with disguised face attacks. It has images of 1000 subjects. A total of 11,155 face images of real world disguise variants obtained from internet sources, formed this dataset. Bhattacharjee et al. [55] created a new Customised Silicon Mask Attack Dataset (CS-MAD) and verified the vulnerability of face biometric system using the dataset. The boost in technology made the manufacturing process of mask easier and cheaper and a number of recent datasets incorporate 3D attacks. Different mask attack datasets are described in Table. 8.

Table 8: 3D mask datasets

Database	**Year**	**Subject**	**Sample**	**Material**
3DMAD [136]	2013	17	255	Paper, hard resin
3DFS-DB [135]	2016	26	520	Plastic
HKBU-MARs [137]	2016	12	1008	Rigid (Two different manufactures)
BRSU [139]	2016	137	141	Silicon, plastic, resin, latex
SMAD [143]	2017	From internet	130	Silicon
MLFP [133]	2017	10	1350	Latex, paper
ERPA [131]	2017	5	86	Resin, silicone
WMCA [51]	2019	72	1679	Rigid, silicone, paper
WFFD [151]	2019	745	2300	Wax figure
CIGIT-PPM [119]	2019	72	93358	Leather, rubber, plastic
3DMA [146]	2019	115	920	48 Variations of masks

Zhang et al. [148] developed a new dataset, CASIA-SURF which was larger than existing datasets in size. The dataset consists of three modalities which are VIS, IR and depth. It has 21,000 sample videos from 1000 subjects. The authors of [147] formed a novel Age Induced Makeup (AIM) dataset. 456 samples using age progressive makeup type from 75 subjects were considered while forming the dataset. Liu et al. [156] formed a Spoof in the Wild (SiW) dataset introducing more spoofing medium and recording settings with photos of 165 subjects. The authors of [146] developed a dataset for 3D Mask Attacks (3DMA) based on VIS and NIR. Xiao et al. developed this dataset in order to apply more variance in lighting distance and illumination deploying various methods. 920 videos of 67 subjects were included in the dataset. There were 48 3D mask variants used to create this dataset.

Emphasizing on video replay attack, Timoshenko et al. created a larger dataset. The Large Crowd Collected Facial Anti-Spoofing Database (LCC FASD) in [149] has more variance in devices deployed for recording and replay. The dataset has 1942 real faces and 16885 attack samples. In [150], the authors introduced a novel dataset Pattern Recognition Face Spoofing Advancement Dataset (PR-FSAD) for spoof detection which emphasizes on variations in angle and distance. 42,480 real and 84,960 fake samples from 30 subjects used to construct the dataset. A new dataset, Digital Forensic - Face Presentation Attack Detection (DF-FPAD) was created for the evaluation process of a presentation attack detection framework using this textural noise in [157]. The dataset was made using higher quality images of fake and genuine faces under controlled conditions.

6. Evaluation Metrics

Face PAD is commonly considered as a binary classification problem. Various performance associated metrics are used to evaluate the performance. Chingovska et al. detailed about measuring face PAD as a binary classification problem [158]. Since these binary classification systems are provided with two classes of input, they normally termed as positive and negative classes. Their performance is evaluated by the types of errors committed and the method to measure them. False Positive and False Negative are the errors exhibited by the binary classification systems. Normally recorded error rates are False Positive Rate (FPR) and False Negative Rate (FNR). FPR is the ratio of FP to the total number of negative samples and FNR is the ratio of FN to the total number of positive samples.

In biometric verification systems, the performance relies upon acceptance or rejection of the sample. So the terms False Positive Rate (FPR) and False Negative Rate (FNR) are replaced by False Acceptance Rate (FAR) and False Rejection Rate (FRR), respectively [159]. As there is matching process involved in the verification task, FAR and FRR are often described as False Match Rate (FMR) and False Non-Match Rate (FNMR) [160]. Anti-spoofing systems function on the concept of acceptance and rejection. So usually PAD systems use FRR and FAR. The ratio of incorrectly accepted spoofing attacks defines FAR, whereas FRR stands for the ratio of incorrectly rejected real accesses [158].

Presentation Attack Detection (PAD) follows ISO/IEC DIS 30107-3:2017 [161] to evaluate the performance of the PAD systems [33]. Authors of [5] described evaluation metrics used for testing different scenarios in a PAD system. The most commonly used metric in anti-spoofing scenarios is Half Total Error Rate (HTER) [158]. HTER is found out by calculating the average of FRR (ratio of incorrectly rejected genuine score) and FAR (ratio of incorrectly accepted zero-effort impostor). FAR is associated with SFAR (ratio of incorrectly accepted spoof attacks). PAD methods used Equal Error Rate (EER) to test reliability [5]. EER is a specific value of HTER at which FAR and FRR have equal values.

While evaluating some methods, metrics mentioned as per ISO standard in [161] were used. They were Attack Presentation Classification Error Rate (APCER), Normal Presentation Classification Error Rate (NPCER) and Average Classification Error Rate (ACER). NPCER is identical to Bona fide Presentation Classification Error Rate (BPCER). A Face PAD is evaluated

Table 9: Commonly used evaluation metrics in face PAD

Metrics		Equation
False Acceptance Rate	FAR	$\frac{FP}{Fake\ samples}$
False Rejection Rate	FRR	$\frac{FN}{Genuine\ samples}$
Equal Error Rate	EER	$(FRR = FAR)$
Half Total Error Rate	HTER	$\frac{FAR+FRR}{2}$
Attack Presentation Classification Error Rate	APCER	$\frac{FP}{FP+TN}$
Bona fide Presentation Classification Error Rate	BPCER	$\frac{FN}{FN+TP}$
Average Classification Error Rate	ACER	$\frac{APCER+BPCER}{2}$

in terms of classification of attacks and real face, intra dataset performance and cross-dataset performance [17]. BPCER and APCER measures bona fide and attack classification error rates respectively. ACER evaluates the intra dataset performance, whereas HTER scales cross-dataset performance [161]. Commonly used metrics [37, 14, 5] in face anti-spoofing are listed in Table. 9.

7. Conclusion and future directions

Presentation attacks continue to pose a challenge for the research community despite the recent and significant progress in the development of detection methods. Methods such as anomaly detection, domain generalisation, few-shot learning, zero-shot learning and others have shown some promising results. In this paper, we have presented an extensive, in-depth review of the most recent literature with an emphasis on deep learning-based methods. We have provided context for this with a comprehensive review of existing presentation attack methods, and critical evaluation of recent datasets and evaluation metrics.

Despite the recent progress in presentation attacks detection methods, unseen attack detection is still considered a challenging problem. Existing methods showed promising results when evaluated using specific type of attacks under controlled environment or using public datasets. PAD models trained used predefined attacks also show promising results, however, such models tend to be biased toward these type of attacks [162]. While machine learning models perform well on samples taken from within the same distribution as the training set, that performance is not maintained across different datasets or in new conditions. In other words, generalising performance across wide range of attacks and across different datasets is still considered an inherently challenging problem. This can be partly attributed to common computer vision challenges such as distance of the subject to the camera, image resolution, light [88], pose variations and others. This suggests strongly that, PAD in an uncontrolled environment requires further research efforts [21, 163].

One of the key challenges to progress research and development of PAD methods is the large number of ways that such attacks can be performed. It remains impractical to compile a dataset that captures all current attack variation regardless of its type (e.g. 2D, 3D attacks). It is impossible to predict the varieties of attack that new technological advances will bring in the future. The literature shows that compared to existing 2D attack datasets, 3D attack datasets and multi-spectral datasets are scarce with fewer subjects to compare to image classification and face recognition datasets. More datasets in the public domain are required to progress research in this area. In particular, datasets that capture novel attacks using recording devices, and other new emerging technologies [148].

The inclusion of temporal features, such as motion or rPPG, for auxiliary supervision is a another challenging task in face PAD. The majority of auxiliary methods in face PAD used spatial features, especially depth as an auxiliary feature. These have considered a single frame for detection. Limited research has been conducted to utilise temporal features for auxiliary supervision. This may be partly attributed to computer processing requirements and the need for rapid processing in face recognition systems. Multiple frames with longer duration have to be processed to deploy temporal features for auxiliary supervision. Hence, multiple frame-based models increase processing time within the face recognition systems [112]. As technology advances, however, temporal features might increase accuracy in PAD, and this research area should not be neglected.

Remodeling face presentation attack detection as one class classification approach has provided impressive results in unseen attack detection. Hence, this approach is a promising future research direction. Delving further into into anomaly detection, few-shot learning, zero-shot learning, and domain generalisation is recommended for enhancing unseen attack detection. Combining this with further investigation into auxiliary supervision with more spatial and temporal features would provide a powerful, new research direction. Recent research has investigated multi-spectral data augmentation using image translation and GANs. This has provided new methods which utilize multi-spectral cues without the need for physical auxiliary sensors. GANs have also been used for learning generalised features over multiple domains in feature space. Hence, further study with GANs in anti-spoofing might provide some way of generalising presentation attack detection over unseen attacks.

References

[1] I. Stylios, S. Kokolakis, O. Thanou, S. Chatzis, Behavioral biometrics & continuous user authentication on mobile devices: A survey, Information Fusion 66 76–99.

[2] D. R. Kisku, R. D. Rakshit, Face spoofing and counter-spoofing: A survey of state-of-the-art algorithms, Transactions on Machine Learning and Artificial Intelligence 5 (2) (2017) 31–31.

[3] N. Abudarham, L. Shkiller, G. Yovel, Critical features for face recognition, Cognition 182 (2019) 73–83.

[4] J. Yang, P. Ren, D. Zhang, D. Chen, F. Wen, H. Li, G. Hua, Neural aggregation network for video face recognition, in: Proceedings of the IEEE conference on computer vision and pattern recognition, 2017, pp. 4362–4371.

[5] R. Ramachandra, C. Busch, Presentation attack detection methods for face recognition systems: A comprehensive survey, ACM Computing Surveys (CSUR) 50 (1) (2017) 1–37.

[6] I. Chingovska, N. Erdogmus, A. Anjos, S. Marcel, Face recognition systems under spoofing attacks, in: Face Recognition Across the Imaging Spectrum, Springer, 2016, pp. 165–194.

[7] S. Soltanpour, B. Boufama, Q. J. Wu, A survey of local feature methods for 3d face recognition, Pattern Recognition 72 (2017) 391–406.

[8] A. Lumini, L. Nanni, Overview of the combination of biometric matchers, Information Fusion 33 (2017) 71–85.

[9] S. Dargan, M. Kumar, A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities, Expert Systems with Applications 143 (2020) 113114.

[10] J. Hernandez-Ortega, J. Fierrez, A. Morales, J. Galbally, Introduction to face presentation attack detection, in: Handbook of Biometric Anti-Spoofing, Springer, 2019, pp. 187–206.

[11] N. Kohli, D. Yadav, A. Noore, Face verification with disguise variations via deep disguise recognizer, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2018, pp. 17–24.

[12] C. Rathgeb, P. Drozdowski, C. Busch, Detection of makeup presentation attacks based on deep face representations, arXiv preprint arXiv:2006.05074 (2020).

[13] R. Singh, M. Vatsa, H. S. Bhatt, S. Bharadwaj, A. Noore, S. S. Nooreyezdan, Plastic surgery: A new dimension to face recognition, IEEE Transactions on Information Forensics and Security 5 (3) (2010) 441–448.

[14] L. Souza, L. Oliveira, M. Pamplona, J. Papa, How far did we get in face spoofing detection?, Engineering Applications of Artificial Intelligence 72 (2018) 368–381.

[15] S. Marcel, M. S. Nixon, S. Z. Li, Handbook of biometric anti-spoofing, Vol. 1, Springer, 2014.

[16] D. Wen, H. Han, A. K. Jain, Face spoof detection with image distortion analysis, IEEE Transactions on Information Forensics and Security 10 (4) (2015) 746–761.

[17] A. Jourabloo, Y. Liu, X. Liu, Face de-spoofing: Anti-spoofing via noise modeling, in: Proceedings of the European Conference on Computer Vision (ECCV), 2018, pp. 290–306.

[18] K. Patel, H. Han, A. K. Jain, Secure face unlock: Spoof detection on smartphones, IEEE transactions on information forensics and security 11 (10) (2016) 2268–2283.

[19] S. Kumar, S. Singh, J. Kumar, A comparative study on face spoofing attacks, in: 2017 International Conference on Computing, Communication and Automation (ICCCA), IEEE, 2017, pp. 1104–1108.

[20] R. Kaur, P. Mann, Techniques of face spoof detection: a review, Int. J. Comput. Appl 164 (1) (2017) 29–33.

[21] A. Rattani, R. Derakhshani, A survey of mobile face biometrics, Computers & Electrical Engineering 72 (2018) 39–52.

[22] R. Munir, R. A. Khan, An extensive review on spectral imaging in biometric systems: Challenges & advancements, Journal of Visual Communication and Image Representation 65 (2019) 102660.

[23] J. Määttä, A. Hadid, M. Pietikäinen, Face spoofing detection from single images using micro-texture analysis, in: 2011 international joint conference on Biometrics (IJCB), IEEE, 2011, pp. 1–7.

[24] I. Chingovska, A. Anjos, S. Marcel, On the effectiveness of local binary patterns in face anti-spoofing, in: 2012 BIOSIG-proceedings of the international conference of biometrics special interest group (BIOSIG), IEEE, 2012, pp. 1–7.

[25] K. Sundararajan, D. L. Woodard, Deep learning for biometrics: A survey, ACM Computing Surveys (CSUR) 51 (3) (2018) 1–34.

[26] O. Kähm, N. Damer, 2d face liveness detection: An overview, in: 2012 BIOSIG-Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG), IEEE, 2012, pp. 1–12.

[27] J. Galbally, S. Marcel, J. Fierrez, Biometric antispoofing methods: A survey in face recognition, IEEE Access 2 (2014) 1530–1552.

[28] A. Hadid, Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2014, pp. 113–118.

[29] I. A. Ghaffar, M. N. H. Mohd, Presentation attack detection for face recognition on smartphones: A comprehensive review, Journal of Telecommunication, Electronic and Computer Engineering (JTEC) 9 (3-8) (2017) 33–38.

[30] A. Mohammadi, S. Bhattacharjee, S. Marcel, Deeply vulnerable: a study of the robustness of face recognition to presentation attacks, Iet Biometrics 7 (1) (2017) 15–26.

[31] E. A. Raheem, S. M. S. Ahmad, W. A. W. Adnan, Insight on face liveness detection: A systematic literature review., International Journal of Electrical & Computer Engineering (2088-8708) 9 (2019).

[32] B. Wu, M. Pan, Y. Zhang, A review of face anti-spoofing and its applications in china, in: International Conference on Harmony Search Algorithm, Springer, 2019, pp. 35–43.

[33] S. Bhattacharjee, A. Mohammadi, A. Anjos, S. Marcel, Recent advances in face presentation attack detection, in: Handbook of Biometric Anti-Spoofing, Springer, 2019, pp. 207–228.

[34] M. T. S. K. kalihal Asst, J. Kaur, A review on different face spoof detection techniques in biometric systems (2019).

[35] S. Jia, G. Guo, Z. Xu, A survey on 3d mask presentation attack detection and countermeasures, Pattern Recognition 98 (2020) 107032.

[36] S. Jia, G. Guo, Z. Xu, Q. Wang, Face presentation attack detection in mobile scenarios: A comprehensive evaluation, Image and Vision Computing 93 (2020) 103826.

[37] A. Liu, X. Li, J. Wan, Y. Liang, S. Escalera, H. J. Escalante, M. Madadi, Y. Jin, Z. Wu, X. Yu, et al., Cross-ethnicity face anti-spoofing recognition challenge: A review, IET Biometrics.

[38] T. I. Dhamecha, A. Nigam, R. Singh, M. Vatsa, Disguise detection and face recognition in visible and thermal spectrums, in: 2013 International Conference on Biometrics (ICB), IEEE, 2013, pp. 1–8.

[39] K. Kotwal, Z. Mostaani, S. Marcel, Detection of age-induced makeup attacks on face recognition systems using multi-layer deep features, IEEE Transactions on Biometrics, Behavior, and Identity Science 2 (1) (2019) 15–25.

[40] R. Singh, A. Agarwal, M. Singh, S. Nagpal, M. Vatsa, On the robustness of face recognition algorithms against attacks and bias, in: Proceedings of the AAAI Conference on Artificial Intelligence, Vol. 34, 2020, pp. 13583–13589.

[41] B. Zhang, B. Tondi, M. Barni, Adversarial examples for replay attacks against cnn-based face recognition with anti-spoofing capability, Computer Vision and Image Understanding 197 (2020) 102988.

[42] D. Deb, X. Liu, A. K. Jain, Faceguard: A self-supervised defense against adversarial face images, arXiv e-prints (2020) arXiv–2011.

[43] T. Yang, X. Zhao, X. Wang, H. Lv, Evaluating facial recognition web services with adversarial and synthetic samples, Neurocomputing 406 (2020) 378–385.

[44] M. Sharif, S. Bhagavatula, L. Bauer, M. K. Reiter, Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition, in: Proceedings of the 2016 acm sigsac conference on computer and communications security, 2016, pp. 1528–1540.

[45] M. Sharif, S. Bhagavatula, L. Bauer, M. K. Reiter, A general framework for adversarial examples with objectives, ACM Transactions on Privacy and Security (TOPS) 22 (3) (2019) 1–30.

[46] Z. Zhou, D. Tang, X. Wang, W. Han, X. Liu, K. Zhang, Invisible mask: Practical attacks on face recognition with infrared, arXiv e-prints (2018) arXiv–1803.

[47] D.-L. Nguyen, S. S. Arora, Y. Wu, H. Yang, Adversarial light projection attacks on face recognition systems: A feasibility study, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, 2020, pp. 814–815.

[48] M. Singh, R. Singh, A. Ross, A comprehensive overview of biometric fusion, Information Fusion 52 (2019) 187–205.

[49] R. Tolosana, M. Gomez-Barrero, C. Busch, J. Ortega-Garcia, Biometric presentation attack detection: Beyond the visible spectrum, IEEE Transactions on Information Forensics and Security 15 (2019) 1261–1275.

[50] M. R. Hasan, S. H. Mahmud, X. Y. Li, Face anti-spoofing using texture-based techniques and filtering methods, in: Journal of Physics: Conference Series, Vol. 1229, IOP Publishing, 2019, p. 012044.

[51] A. George, Z. Mostaani, D. Geissenbuhler, O. Nikisins, A. Anjos, S. Marcel, Biometric face presentation attack detection with multi-channel convolutional neural network, IEEE Transactions on Information Forensics and Security 15 (2019) 42–55.

[52] X. Tan, Y. Li, J. Liu, L. Jiang, Face liveness detection from a single image with sparse low rank bilinear discriminative model, in: European Conference on Computer Vision, Springer, 2010, pp. 504–517.

[53] R. Ramachandra, M. Stokkenes, A. Mohammadi, S. Venkatesh, K. Raja, P. Wasnik, E. Poiret, S. Marcel, C. Busch, Smartphone multi-modal biometric authentication: Database and evaluation, arXiv preprint arXiv:1912.02487 (2019).

[54] R. Ramachandra, S. Venkatesh, K. B. Raja, S. Bhattacharjee, P. Wasnik, S. Marcel, C. Busch, Custom silicone face masks: Vulnerability of commercial face recognition systems & presentation attack detection, in: 2019 7th International Workshop on Biometrics and Forensics (IWBF), IEEE, 2019, pp. 1–6.

[55] S. Bhattacharjee, A. Mohammadi, S. Marcel, Spoofing deep face recognition with custom silicone masks, in: 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), IEEE, 2018, pp. 1–7.

[56] A. G. Yılmaz, U. Turhal, V. V. Nabiyev, Effect of feature selection with meta-heuristic optimization methods on face spoofing detection, Journal of Modern Technology and Engineering 5 (1) (2020) 48–59.

[57] A. Alotaibi, A. Mahmood, Deep face liveness detection based on nonlinear diffusion using convolution neural network, Signal, Image and Video Processing 11 (4) (2017) 713–720.

[58] S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, A. T. Ho, Detection of face spoofing using visual dynamics, IEEE transactions on information forensics and security 10 (4) (2015) 762–777.

[59] G. Arora, K. Tiwari, P. Gupta, Liveness and threat aware selfie face recognition, in: Selfie Biometrics, Springer, 2019, pp. 197–210.

[60] M. Singh, A. Arora, A novel face liveness detection algorithm with multiple liveness indicators, Wireless Personal Communications 100 (4) (2018) 1677–1687.

[61] M. Killioğlu, M. Taşkiran, N. Kahraman, Anti-spoofing in face recognition with liveness detection using pupil tracking, in: 2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI), IEEE, 2017, pp. 000087–000092.

[62] 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.

[63] X. Li, J. Komulainen, G. Zhao, P.-C. Yuen, M. Pietikäinen, Generalized face anti-spoofing by detecting pulse from face videos, in: 2016 23rd International Conference on Pattern Recognition (ICPR), IEEE, 2016, pp. 4244–4249.

[64] S.-Y. Wang, S.-H. Yang, Y.-P. Chen, J.-W. Huang, Face liveness detection based on skin blood flow analysis, symmetry 9 (12) (2017) 305.

[65] B. Lin, X. Li, Z. Yu, G. Zhao, Face liveness detection by rppg features and contextual patch-based cnn, in: Proceedings of the 2019 3rd International Conference on Biometric Engineering and Applications, 2019, pp. 61–68.

[66] J. Komulainen, A. Hadid, M. Pietikäinen, Context based face anti-spoofing, in: 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), IEEE, 2013, pp. 1–8.

[67] J. Yang, Z. Lei, S. Liao, S. Z. Li, Face liveness detection with component dependent descriptor, in: 2013 International Conference on Biometrics (ICB), IEEE, 2013, pp. 1–6.

[68] Z. Boulkenafet, J. Komulainen, A. Hadid, Face antispoofing using speeded-up robust features and fisher vector encoding, IEEE Signal Processing Letters 24 (2) (2016) 141–145.

[69] B. Peixoto, C. Michelassi, A. Rocha, Face liveness detection under bad illumination conditions, in: 2011 18th IEEE International Conference on Image Processing, IEEE, 2011, pp. 3557–3560.

[70] X. Tu, H. Zhang, M. Xie, Y. Luo, Y. Zhang, Z. Ma, Deep transfer across domains for face antispoofing, Journal of Electronic Imaging 28 (4) (2019) 043001.

[71] M. Gogate, K. Dashtipour, A. Adeel, A. Hussain, Cochleanet: A robust language-independent audio-visual model for real-time speech enhancement, Information Fusion 63 (2020) 273 – 285.

[72] A. Adeel, M. Gogate, A. Hussain, W. M. Whitmer, Lip-reading driven deep learning approach for speech enhancement, IEEE Transactions on Emerging Topics in Computational Intelligence (2019) 1–10.

[73] M. Mahmud, M. S. Kaiser, A. Hussain, S. Vassanelli, Applications of deep learning and reinforcement learning to biological data, IEEE Transactions on Neural Networks and Learning Systems 29 (6) (2018) 2063–2079.

[74] C. Ieracitano, A. Adeel, F. C. Morabito, A. Hussain, A novel statistical analysis and autoencoder driven intelligent intrusion detection approach, Neurocomputing 387 (2020) 51 – 62.

[75] S. Pouyanfar, S. Sadiq, Y. Yan, H. Tian, Y. Tao, M. P. Reyes, M.-L. Shyu, S.-C. Chen, S. Iyengar, A survey on deep learning: Algorithms, techniques, and applications, ACM Computing Surveys (CSUR) 51 (5) (2018) 1–36.

[76] Y. A. U. Rehman, L. M. Po, M. Liu, Livenet: Improving features generalization for face liveness detection using convolution neural networks, Expert Systems with Applications 108 (2018) 159 – 169.

[77] F.-M. Chen, C. Wen, K. Xie, F.-Q. Wen, G.-Q. Sheng, X.-G. Tang, Face liveness detection: fusing colour texture feature and deep feature, IET Biometrics 8 (6) (2019) 369–377.

[78] J. Yosinski, J. Clune, Y. Bengio, H. Lipson, How transferable are features in deep neural networks?, in: Advances in neural information processing systems, 2014, pp. 3320–3328.

[79] C. Nagpal, S. R. Dubey, A performance evaluation of convolutional neural networks for face anti spoofing, in: 2019 International Joint Conference on Neural Networks (IJCNN), IEEE, 2019, pp. 1–8.

[80] O. Lucena, A. Junior, V. Moia, R. Souza, E. Valle, R. Lotufo, Transfer learning using convolutional neural networks for face anti-spoofing, in: International Conference Image Analysis and Recognition, Springer, 2017, pp. 27–34.

[81] J. Yang, Z. Lei, D. Yi, S. Z. Li, Person-specific face antispoofing with subject domain adaptation, IEEE Transactions on Information Forensics and Security 10 (4) (2015) 797–809.

[82] O. Nikisins, A. George, S. Marcel, Domain adaptation in multi-channel autoencoder based features for robust face anti-spoofing, in: International Conference on Biometrics 2019, IEEE, no. CONF, 2019.

[83] Z. Yu, J. Wan, Y. Qin, X. Li, S. Li, G. Zhao, Nas-fas: Static-dynamic central difference network search for face anti-spoofing., IEEE Transactions on Pattern Analysis and Machine Intelligence (2020).

[84] G. Wang, H. Han, S. Shan, X. Chen, Improving cross-database face presentation attack detection via adversarial domain adaptation, in: International Conference on Biometrics (ICB), 2019.

[85] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, Y. Bengio, Generative adversarial nets, in: Z. Ghahramani, M. Welling, C. Cortes, N. D. Lawrence, K. Q. Weinberger (Eds.), Advances in Neural Information Processing Systems 27, Curran Associates, Inc., 2014, pp. 2672–2680.

[86] G. Wang, H. Han, S. Shan, X. Chen, Unsupervised adversarial domain adaptation for cross-domain face presentation attack detection, IEEE Transactions on Information Forensics and Security 16 (2020) 56–69.

[87] F. Zhou, C. Gao, F. Chen, C. Li, X. Li, F. Yang, Y. Zhao, Face anti-spoofing based on multi-layer domain adaptation, in: 2019 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), IEEE, 2019, pp. 192–197.

[88] A. Mohammadi, S. Bhattacharjee, S. Marcel, Domain adaptation for generalization of face presentation attack detection in mobile settengs with minimal information, in: ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2020, pp. 1001–1005.

[89] A. Costa-Pazo, D. Jiménez-Cabello, E. Vázquez-Fernández, J. L. Alba-Castro, R. J. López-Sastre, Generalized presentation attack detection: a face anti-spoofing evaluation proposal, in: 2019 International Conference on Biometrics (ICB), IEEE, 2019, pp. 1–8.

[90] S. Saha, W. Xu, M. Kanakis, S. Georgoulis, Y. Chen, D. P. Paudel, L. Van Gool, Domain agnostic feature learning for image and video based face anti-spoofing, in: 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), IEEE, 2020, pp. 3490–3499.

[91] G. Wang, H. Han, S. Shan, X. Chen, Cross-domain face presentation attack detection via multi-domain disentangled representation learning, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020, pp. 6678–6687.

[92] R. Shao, X. Lan, J. Li, P. C. Yuen, Multi-adversarial discriminative deep domain generalization for face presentation attack detection, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2019, pp. 10023–10031.

[93] Y. Jia, J. Zhang, S. Shan, X. Chen, Single-side domain generalization for face anti-spoofing, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020, pp. 8484–8493.

[94] K.-Y. Zhang, T. Yao, J. Zhang, Y. Tai, S. Ding, J. Li, F. Huang, H. Song, L. Ma, Face anti-spoofing via disentangled representation learning, in: European Conference on Computer Vision, Springer, 2020, pp. 641–657.

[95] S. R. Arashloo, J. Kittler, W. Christmas, An anomaly detection approach to face spoofing detection: A new formulation and evaluation protocol, IEEE Access 5 (2017) 13868–13882.

[96] S. R. Arashloo, J. Kittler, Client-specific anomaly detection for face presentation attack detection, arXiv preprint arXiv:1807.00848 (2018).

[97] O. Nikisins, A. Mohammadi, A. Anjos, S. Marcel, On effectiveness of anomaly detection approaches against unseen presentation attacks in face anti-spoofing, in: 2018 International Conference on Biometrics (ICB), IEEE, 2018, pp. 75–81.

[98] S. Fatemifar, S. R. Arashloo, M. Awais, J. Kittler, Spoofing attack detection by anomaly detection, in: ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2019, pp. 8464–8468.

[99] S. Fatemifar, M. Awais, S. R. Arashloo, J. Kittler, Combining multiple one-class classifiers for anomaly based face spoofing attack detection, in: 2019 International Conference on Biometrics (ICB), IEEE, 2019, pp. 1–7.

[100] D. Pérez-Cabo, D. Jiménez-Cabello, A. Costa-Pazo, R. J. López-Sastre, Deep anomaly detection for generalized face anti-spoofing, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2019, pp. 0–0.

[101] L. Abduh, I. Ivrissimtzis, Use of in-the-wild images for anomaly detection in face anti-spoofing, arXiv (2020) arXiv–2006.

[102] Z. Li, H. Li, K.-Y. Lam, A. C. Kot, Unseen face presentation attack detection with hypersphere loss, in: ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2020, pp. 2852–2856.

[103] H. Feng, Z. Hong, H. Yue, Y. Chen, K. Wang, J. Han, J. Liu, E. Ding, Learning generalized spoof cues for face anti-spoofing, arXiv preprint arXiv:2005.03922 (2020).

[104] Y. Baweja, P. Oza, P. Perera, V. M. Patel, Anomaly detection-based unknown face presentation attack detection, in: 2020 IEEE International Joint Conference on Biometrics (IJCB), IEEE, 2020, pp. 1–9.

[105] Y. Wang, Q. Yao, J. T. Kwok, L. M. Ni, Generalizing from a few examples: A survey on few-shot learning, ACM Computing Surveys (CSUR) 53 (3) (2020) 1–34.

[106] Y. Qin, C. Zhao, X. Zhu, Z. Wang, Z. Yu, T. Fu, F. Zhou, J. Shi, Z. Lei, Learning meta model for zero-and few-shot face antispoofing, Association for Advancement of Artificial Intelligence (AAAI) (2020).

[107] Y. Liu, J. Stehouwer, A. Jourabloo, X. Liu, Deep tree learning for zero-shot face anti-spoofing, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2019, pp. 4680–4689.

[108] Y. Liu*, A. Jourabloo*, X. Liu, Learning deep models for face anti-spoofing: Binary or auxiliary supervision, in: In Proceeding of IEEE Computer Vision and Pattern Recognition, Salt Lake City, UT, 2018.

[109] Y. Atoum, Y. Liu, A. Jourabloo, X. Liu, Face anti-spoofing using patch and depth-based cnns, in: 2017 IEEE International Joint Conference on Biometrics (IJCB), IEEE, 2017, pp. 319–328.

[110] A. George, S. Marcel, Deep pixel-wise binary supervision for face presentation attack detection, in: 2019 International Conference on Biometrics (ICB), IEEE, 2019, pp. 1–8.

[111] Z. Wang, C. Zhao, Y. Qin, Q. Zhou, G. Qi, J. Wan, Z. Lei, Exploiting temporal and depth information for multi-frame face anti-spoofing, arXiv preprint arXiv:1811.05118 (2018).

[112] Z. Yu, C. Zhao, Z. Wang, Y. Qin, Z. Su, X. Li, F. Zhou, G. Zhao, Searching central difference convolutional networks for face anti-spoofing, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020, pp. 5295–5305.

[113] Z. Yu, Y. Qin, X. Li, Z. Wang, C. Zhao, Z. Lei, G. Zhao, Multi-modal face anti-spoofing based on central difference networks, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, 2020, pp. 650–651.

[114] Z. Yu, X. Li, X. Niu, J. Shi, G. Zhao, Face anti-spoofing with human material perception, in: European Conference on Computer Vision, Springer, 2020, pp. 557–575.

[115] T. Kim, Y. Kim, I. Kim, D. Kim, Basn: Enriching feature representation using bipartite auxiliary supervisions for face anti-spoofing, in: Proceedings of the IEEE International Conference on Computer Vision Workshops, 2019, pp. 0–0.

[116] Y. Liu, J. Stehouwer, A. Jourabloo, Y. Atoum, X. Liu, Presentation attack detection for face in mobile phones, in: Selfie Biometrics, Springer, 2019, pp. 171–196.

[117] Y. A. U. Rehman, L.-M. Po, M. Liu, Slnet: Stereo face liveness detection via dynamic disparity-maps and convolutional neural network, Expert Systems with Applications 142 (2020) 113002.

[118] X. Yang, W. Luo, L. Bao, Y. Gao, D. Gong, S. Zheng, Z. Li, W. Liu, Face anti-spoofing: Model matters, so does data, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2019, pp. 3507–3516.

[119] F. Jiang, P. Liu, X. Zhou, Multilevel fusing paired visible light and near-infrared spectral images for face anti-spoofing, Pattern Recognition Letters 128 (2019) 30 – 37.

[120] A. George, Z. Mostaani, D. Geissenbuhler, O. Nikisins, A. Anjos, S. Marcel, Biometric face presentation attack detection with multi-channel convolutional neural network, IEEE Transactions on Information Forensics and Security 15 (2020) 42–55.

[121] K. Kotwal, S. Bhattacharjee, S. Marcel, Multispectral deep embeddings as a countermeasure to custom silicone mask presentation attacks, IEEE Transactions on Biometrics, Behavior, and Identity Science 1 (4) (2019) 238–251.

[122] H. Chen, G. Hu, Z. Lei, Y. Chen, N. M. Robertson, S. Z. Li, Attention-based two-stream convolutional networks for face spoofing detection, IEEE Transactions on Information Forensics and Security 15 (2019) 578–593.

[123] Y. Fan, Y. Shi, X. Wang, H. Yi, Research on liveness detection algorithms based on deep learning, in: 2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS), IEEE, 2019, pp. 1–6.

[124] G. Wang, C. Lan, H. Han, S. Shan, X. Chen, Multi-modal face presentation attack detection via spatial and channel attentions, in: 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), IEEE Computer Society, 2019, pp. 1584–1590.

[125] F. Jiang, P. Liu, X. Shao, X. Zhou, Face anti-spoofing with generated near-infrared images, Multimedia Tools and Applications (2020) 1–25.

[126] S. Liu, Y. Song, M. Zhang, J. Zhao, S. Yang, K. Hou, An identity authentication method combining liveness detection and face recognition, Sensors 19 (21) (2019) 4733.

[127] Y. Hong, U. Hwang, J. Yoo, S. Yoon, How generative adversarial networks and their variants work: An overview, ACM Computing Surveys (CSUR) 52 (1) (2019) 1–43.

[128] A. Anjos, I. Chingovska, S. Marcel, Anti-spoofing: Face databases, Tech. rep., Springer US (2014).

[129] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, S. Z. Li, A face antispoofing database with diverse attacks, in: 2012 5th IAPR international conference on Biometrics (ICB), IEEE, 2012, pp. 26–31.

[130] A. Dantcheva, C. Chen, A. Ross, Can facial cosmetics affect the matching accuracy of face recognition systems?, in: 2012 IEEE Fifth international conference on biometrics: theory, applications and systems (BTAS), IEEE, 2012, pp. 391–398.

[131] S. Bhattacharjee, S. Marcel, What you can't see can help you-extended-range imaging for 3d-mask presentation attack detection, in: 2017 International Conference of the Biometrics Special Interest Group (BIOSIG), IEEE, 2017, pp. 1–7.

[132] C. Chen, A. Dantcheva, A. Ross, Automatic facial makeup detection with application in face recognition, in: 2013 international conference on biometrics (ICB), IEEE, 2013, pp. 1–8.

[133] A. Agarwal, D. Yadav, N. Kohli, R. Singh, M. Vatsa, A. Noore, Face presentation attack with latex masks in multispectral videos, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2017, pp. 81–89.

[134] R. Raghavendra, K. B. Raja, C. Busch, Presentation attack detection for face recognition using light field camera, IEEE Transactions on Image Processing 24 (3) (2015) 1060–1075.

[135] J. Galbally, R. Satta, Three-dimensional and two-and-a-half-dimensional face recognition spoofing using three-dimensional printed models, IET Biometrics 5 (2) (2016) 83–91.

[136] N. Erdogmus, S. Marcel, Spoofing 2d face recognition systems with 3d masks, in: 2013 International Conference of the BIOSIG Special Interest Group (BIOSIG), IEEE, 2013, pp. 1–8.

[137] S. Liu, B. Yang, P. C. Yuen, G. Zhao, A 3d mask face anti-spoofing database with real world variations, in: Proceedings of the IEEE conference on computer vision and pattern recognition workshops, 2016, pp. 100–106.

[138] A. Costa-Pazo, S. Bhattacharjee, E. Vazquez-Fernandez, S. Marcel, The replay-mobile face presentation-attack database, in: 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), IEEE, 2016, pp. 1–7.

[139] H. Steiner, S. Sporrer, A. Kolb, N. Jung, Design of an active multi-spectral swir camera system for skin detection and face verification, Journal of Sensors 2016 (2016).

[140] R. Raghavendra, K. B. Raja, S. Venkatesh, F. A. Cheikh, C. Busch, On the vulnerability of extended multispectral face recognition systems towards presentation attacks, in: 2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA), IEEE, 2017, pp. 1–8.

[141] C. Chen, A. Dantcheva, T. Swearingen, A. Ross, Spoofing faces using makeup: An investigative study, in: 2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA), IEEE, 2017, pp. 1–8.

[142] Z. Boulkenafet, J. Komulainen, L. Li, X. Feng, A. Hadid, Oulu-npu: A mobile face presentation attack database with real-world variations, in: 2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017), IEEE, 2017, pp. 612–618.

[143] I. Manjani, S. Tariyal, M. Vatsa, R. Singh, A. Majumdar, Detecting silicone mask-based presentation attack via deep dictionary learning, IEEE Transactions on Information Forensics and Security 12 (7) (2017) 1713–1723.

[144] M. Singh, R. Singh, M. Vatsa, N. K. Ratha, R. Chellappa, Recognizing disguised faces in the wild, IEEE Transactions on Biometrics, Behavior, and Identity Science 1 (2) (2019) 97–108.

[145] H. Li, W. Li, H. Cao, S. Wang, F. Huang, A. C. Kot, Unsupervised domain adaptation for face anti-spoofing, IEEE Transactions on Information Forensics and Security 13 (7) (2018) 1794–1809.

[146] J. Xiao, Y. Tang, J. Guo, Y. Yang, X. Zhu, Z. Lei, S. Z. Li, 3dma: A multi-modality 3d mask face anti-spoofing database, in: 2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), IEEE, 2019, pp. 1–8.

[147] K. Kotwal, Z. Mostaani, S. Marcel, Detection of age-induced makeup attacks on face recognition systems using multi-layer deep features, IEEE Transactions on Biometrics, Behavior, and Identity Science 2 (1) (2020) 15–25.

[148] S. Zhang, A. Liu, J. Wan, Y. Liang, G. Guo, S. Escalera, H. J. Escalante, S. Z. Li, Casia-surf: A large-scale multi-modal benchmark for face anti-spoofing, IEEE Transactions on Biometrics, Behavior, and Identity Science (2020) 1–1.

[149] D. Timoshenko, K. Simonchik, V. Shutov, P. Zhelezneva, V. Grishkin, Large crowd collected facial anti-spoofing dataset, in: 2019 Computer Science and Information Technologies (CSIT), IEEE, 2019, pp. 123–126.

[150] J. Y. Bok, K. H. Suh, E. C. Lee, Verifying the effectiveness of new face spoofing db with capture angle and distance, Electronics 9 (4) (2020) 661.

[151] S. Jia, X. Li, C. Hu, Z. Xu, Spoofing and anti-spoofing with wax figure faces, arXiv preprint arXiv:1910.05457 (2019).

[152] A. Liu, Z. Tan, J. Wan, S. Escalera, G. Guo, S. Z. Li, Casia-surf cefa: A benchmark for multi-modal cross-ethnicity face anti-spoofing, in: Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, 2021, pp. 1179–1187.

[153] Y. Zhang, Z. Yin, Y. Li, G. Yin, J. Yan, J. Shao, Z. Liu, Celeba-spoof: Large-scale face anti-spoofing dataset with rich annotations, in: European Conference on Computer Vision, Springer, 2020, pp. 70–85.

[154] T. I. Dhamecha, R. Singh, M. Vatsa, A. Kumar, Recognizing disguised faces: Human and machine evaluation, PloS one 9 (7) (2014).

[155] V. Kushwaha, M. Singh, R. Singh, M. Vatsa, N. Ratha, R. Chellappa, Disguised faces in the wild, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2018, pp. 1–9.

[156] Y. Liu, A. Jourabloo, X. Liu, Learning deep models for face anti-spoofing: Binary or auxiliary supervision, in: Proceedings of the IEEE conference on computer vision and pattern recognition, 2018, pp. 389–398.

[157] H. P. Nguyen, A. Delahaies, F. Retraint, F. Morain-Nicolier, Face presentation attack detection based on a statistical model of image noise, IEEE Access 7 (2019) 175429–175442.

[158] I. Chingovska, A. R. Dos Anjos, S. Marcel, Biometrics evaluation under spoofing attacks, IEEE transactions on Information Forensics and Security 9 (12) (2014) 2264–2276.

[159] J. Galbally, F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, A high performance fingerprint liveness detection method based on quality related features, Future Generation Computer Systems 28 (1) (2012) 311–321.

[160] G. Pan, L. Sun, Z. Wu, S. Lao, Eyeblink-based anti-spoofing in face recognition from a generic webcamera, in: 2007 IEEE 11th International Conference on Computer Vision, IEEE, 2007, pp. 1–8.

[161] Information technology- biometric presentation attack detection- part 3: Testing and reporting, International Organization for Standardization ISO/IEC DIS 30107-3:2017 (2017).

[162] F. Xiong, W. AbdAlmageed, Unknown presentation attack detection with face rgb images, in: 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), IEEE, 2018, pp. 1–9.

[163] F. Peng, L. Qin, M. Long, Face presentation attack detection based on chromatic co-occurrence of local binary pattern and ensemble learning, Journal of Visual Communication and Image Representation 66 (2020) 102746.