Chapter 9
Introduction to Presentation Attack Detection in Face Biometrics and Recent Advances

Javier Hernandez-Ortega, Julian Fierrez, Aythami Morales, and Javier Galbally

Abstract The main scope of this chapter is to serve as an introduction to face presentation attack detection, including key resources and advances in the field in the last few years. The next pages present the different presentation attacks that a face recognition system can confront, in which an attacker presents to the sensor, mainly a camera, a Presentation Attack Instrument (PAI), that is generally a photograph, a video, or a mask, with the target to impersonate a genuine user or to hide the actual identity of the attacker via obfuscation. First, we make an introduction of the current status of face recognition, its level of deployment, and its challenges. In addition, we present the vulnerabilities and the possible attacks that a face recognition system may be exposed to, showing that way the high importance of presentation attack detection methods. We review different types of presentation attack methods, from simpler to more complex ones, and in which cases they could be effective. Then, we summarize the most popular presentation attack detection methods to deal with these attacks. Finally, we introduce public datasets used by the research community for exploring vulnerabilities of face biometrics to presentation attacks and developing effective countermeasures against known PAIs.

J. Hernandez-Ortega (✉) · J. Fierrez (✉) · A. Morales (✉)
School of Engineering, Universidad Autonoma de Madrid, Madrid, Spain
e-mail: javier.hernandezo@uam.es

J. Fierrez
e-mail: julian.fierrez@uam.es

A. Morales
e-mail: aythami.morales@uam.es

J. Galbally (✉)
eu-LISA / European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, Tallinn, Estonia
e-mail: javier.galbally@eulisa.europa.eu

S. Marcel et al. (eds.), *Handbook of Biometric Anti-Spoofing*, Advances in Computer Vision and Pattern Recognition, https://doi.org/10.1007/978-981-19-5288-3_9

9.1 Introduction

Over the last decades, there have been numerous technological advances that helped to bring new possibilities to people in the form of new devices and services. Some years ago, it would have been almost impossible to imagine having in the market devices like current smartphones and laptops, at affordable prices, that allow a high percentage of the population to have their own piece of top-level technology at home, a privilege that historically has been restricted to big companies and research groups.

Thanks to this quick advance in technology, specially in computer science and electronics, it has been possible to broadly deploy biometric systems for the first time. Nowadays, they are present in a high number of scenarios like border access control [1], surveillance [2], smartphone authentication [3], forensics [4], and on-line services like e-commerce and e-learning [5].

Among all the existing biometric characteristics, face recognition is currently one of the most extended. Face has been studied as a mean of recognition since the 60s, acquiring special relevance in the 90s following the evolution of computer vision [6]. Some interesting properties of the interaction of human faces with biometric systems are acquisition at a distance, non-intrusive, and the highly discriminant features of the face to perform identity recognition.

At present, face is one of the biometric characteristics with the highest economical and social impact due to several reasons:

- Face is one of the most largely deployed biometric modes at world level in terms of market quota [7]. Each day more and more manufacturers are including Face Recognition Systems (FRSs) in their products, like Apple with its Face ID technology. The public sector is also starting to use face recognition for a wide range of purposes like demographic analysis, identification, and access control [8].
- Face is adopted in most identification documents such as the ICAO-compliant biometric passport [9] or national ID cards [10].

Given their high level of deployment, attacks having a FRS as their target are not restricted anymore to theoretical scenarios, becoming a real threat. There are all kinds of applications and sensitive information that can be menaced by attackers. Providing each face recognition application with an appropriate level of security, as it is being done with other biometric characteristics, like iris or fingerprint, should be a top priority.

Historically, the main focus of research in face recognition has been given to the improvement of the performance at verification and identification tasks, that means, distinguishing better between subjects using the available information of their faces. To achieve that goal, a FRS should be able to optimize the differences between the facial features of each user and also the similarities among samples of the same user [11, 12]. Within the variability factors that can affect the performance of face recognition systems there are occlusions, low-resolution, different viewpoints, lighting, etc. Improving the performance of recognition systems in the presence of

these variability factors is currently an active and challenging area in face recognition research [13–15].

Contrary to the optimization of their performance, the security vulnerabilities of face recognition systems have been much less studied in the past, and only over the recent few years some attention has been given to detecting different types of attacks [16–18].

Presentation Attacks (PA) can be defined as the presentation of human characteristics or artifacts directly to the input sensor of a biometric system, trying to interfere its normal operation. This category of attacks is highly present in real-world applications of biometrics since the attackers do not need to have access to the internal modules of the recognition system. For example, presenting a high-quality printed face of a legitimate user to a camera can be enough to compromise a face recognition system if it does not implement proper countermeasures against these artifacts.

The target of face Presentation Attack Detection (PAD) systems is the automated determination of presentation attacks. Face PAD methods aim to distinguish between a legitimate face and a Presentation Attack Instrument (PAI) that tries to mimic bona fide biometric traits. For example, a subset of PAD methods, referred to as liveness detection, involves measurement and analysis of anatomical characteristics or of involuntary and voluntary reactions, in order to determine if a biometric sample is being captured from a living subject actually present at the point of capture. By applying liveness detection, a face recognition system can become resilient against many presentation attacks like the printed photo attacks mentioned previously.

The rest of this chapter is organized as follows: Sect. 9.2 overviews the main vulnerabilities of face recognition systems, making a description of several presentation attack approaches. Section 9.3 introduces presentation attack detection techniques. Section 9.4 presents some available public databases for research and evaluation of face presentation attack detection. Section 9.5 discusses different architectures and applications of face PAD. Finally, concluding remarks and future lines of work in face PAD are drawn in Sect. 9.6.

9.2 Vulnerabilities in Face Biometrics

In the present chapter we concentrate on Presentation Attacks, i.e., attacks against the sensor of a FRS [19] (see point V1 in Fig. 9.1). Some relevant properties of these attacks are that they require low information about the attacked system and that they present a high success probability when the FRS is not properly protected.

On the contrary, indirect attacks (points V2-V7 in Fig. 9.1) are those attacks to the inner modules of the FRS, i.e., the preprocessing module, the feature extractor, the classifier, or the enrolling database. A detailed definition of indirect attacks to face systems can be found in [20]. Indirect attacks can be prevented by improving certain points of the FRS [21], like the communication channels, the equipment and infrastructure involved and the perimeter security. The techniques needed for improving those modules are more related to "classical" cybersecurity than to biometric tech-

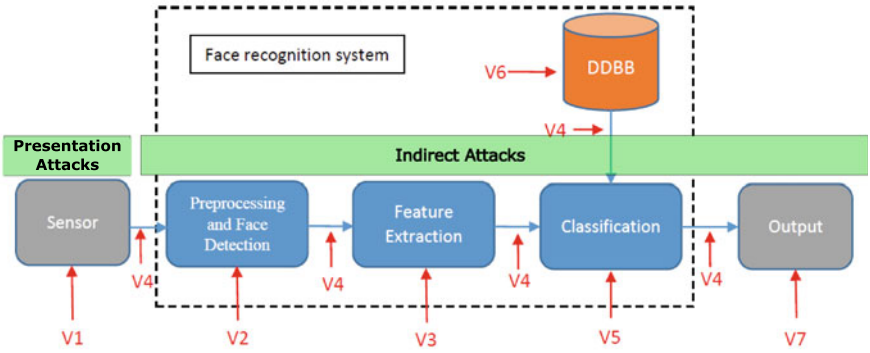

Fig. 9.1 Scheme of a generic biometric system. In this type of system, there exist several modules and points that can be the target of an attack (Vulnerabilities V1 to V7). Presentation attacks are performed at sensor level (V1), without the need of having access to the inner modules of the system. Indirect attacks (V2 to V7) can be performed at the databases, the matcher, the communication channels, etc.; in this type of attack the attacker needs access to the inner modules of the system and in most cases also specific information about their functioning

niques. These attacks and their countermeasures are beyond the scope of this book but should not be underestimated.

Presentation attacks are a purely biometric vulnerability that is not shared with other IT security solutions and that needs specific countermeasures. In these attacks, intruders use some type of artifact, typically artificial (e.g., a face photo, a mask, a synthetic fingerprint, or a printed iris image), or try to mimic the aspect of genuine users (e.g., gait, signature, or facial expression [22]) to present it to the acquisition scanner and fraudulently access the biometric system.

A high amount of biometric data are exposed, (e.g., photographs and videos on social media sites) showing the face, eyes, voice, and behavior of people. Presentation attackers are aware of this reality and take advantage of those sources of information to try to circumvent face recognition systems [23]. This is one of the well-known drawbacks of biometrics: "biometric characteristics are not secrets" [24]. In this context, it is worth noting that the factors that make face an interesting characteristic for person recognition, that is, images that can be taken at a distance and in a non-intrusive way, make it also specially vulnerable to attackers who want to use biometric information in an illicit manner.

In addition to being fairly easy to obtain a face image of the legitimate users, face recognition systems are known to respond weakly to presentation attacks, for example using one of these three categories of attacks:

1. Using a photograph of the user to be impersonated [25].
2. Using a video of the user to be impersonated [26, 27].
3. Building and using a 3D model of the attacked face, for example, an hyper-realistic mask [28].

The success probability of an attack may vary considerably depending on the characteristics of the FRS, for example, if it uses visible light or works in another range of the electromagnetic spectrum (e.g., infra-red lighting), if it has one or several sensors (e.g., 3D sensors, thermal sensors), the resolution, the lighting, and also depending on the characteristics of the PAI: quality of the texture, the appearance, the resolution of the presentation device, the type of support used to present the fake, or the background conditions.

Without implementing presentation attack detection measures most of the state-of-the-art facial biometric systems are vulnerable to simple attacks that a regular person would detect easily. This is the case, for example, of trying to impersonate a subject using a photograph of his face. Therefore, in order to design a secure FRS in a real scenario, for instance for replacing password-based authentication, Presentation Attack Detection (PAD) techniques should be a top priority from the initial planning of the system.

Given the discussion above, it could be stated that face recognition systems without PAD techniques are at clear risk, so a question often rises: What technique(s) should be adopted to secure them? The fact is that counterfeiting this type of threat is not a straightforward problem, as new specific countermeasures need to be developed and adopted whenever a new attack appears.

With the scope of encouraging and boosting the research in presentation attack detection techniques in face biometrics, there are numerous and very diverse initiatives in the form of dedicated tracks, sessions and workshops in biometric-specific and general signal processing conferences [29, 30]; organization of competitions [31–33]; and acquisition of benchmark datasets [27, 28, 34–36] that have resulted in the proposal of new presentation attack detection methods [19, 37]; standards in the area [38, 39]; and patented PAD mechanisms for face recognition systems [40, 41].

9.2.1 Presentation Attack Methods

Typically, a FRS can be spoofed by presenting to the sensor (e.g., a camera) a photograph, a video, or a 3D mask of a targeted person (see Fig. 9.2). There are other possibilities in order to circumvent a FRS, such as using makeup [42, 43] or plastic surgery. However, using photographs and videos is the most common type of attacks due to the high exposition of face (e.g., social media, video-surveillance), and the low cost of high-resolution digital cameras, printers, or digital screens.

Regarding the attack types, a general classification can be done by taking into account the nature and the level of complexity of the PAI used to attack: photo-based, video-based, and mask-based (as can be seen in Fig. 9.2). It must be remarked that this is only a classification of the most common types of attacks, but there are some complex attacks that may not fall specifically into in any of these categories, or that may belong to several categories at the same time. This is the case of DeepFake methods, that are usually defined as techniques able to create fake videos by swapping

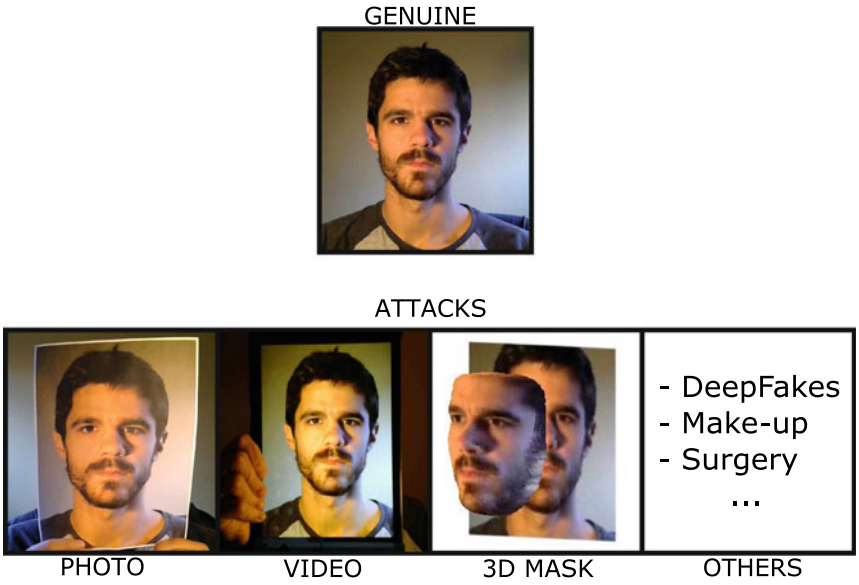

Fig. 9.2 Examples of face presentation attacks: The upper image shows an example of a genuine user, and below it there are some examples of presentation attacks, depending on the PAI shown to the sensor: a photo, a video, a 3D mask, DeepFakes, make-up, surgery, and others

the face of a person with the face of another person, and that could be classified into photo attacks, video attacks, or even mask attacks. In this chapter, we have classified those more complex and special attacks in a category named "Other attacks".

9.2.1.1 Photo Attacks

A photo attack consists in displaying a photograph of the attacked identity to the sensor of the face recognition system [44, 45] (see example in Fig. 9.2).

Photo attacks are the most critical type of attack to be protected from due to several factors. On the one hand, printing color images from the face of the genuine user is really cheap and easy to do. These are usually called print attacks in the literature [46]. Alternatively, the photos can be displayed in the high-resolution screen of a device (e.g., a smartphone, a tablet or a laptop [26, 34, 44]). On the other hand, it is also easy to obtain samples of genuine faces thanks to the recent growth of social media sites like Facebook, Twitter, and Instagram [23]. Additionally, with the price and size reduction experimented by digital cameras in recent years, it is also possible to obtain high-quality photos of a legitimate user simply by using a hidden camera.

Among the photo attack techniques, there are also more complex approaches like photographic masks. This technique consists in printing a photograph of the subject's face and then making holes for the eyes and the mouth [34]. This is a good way to

avoid presentation attack detection techniques based on blink detection and in eyes and mouth movement tracking [47].

Even if these attacks may seem too simple to work in a real scenario, some studies indicate that many state-of-the-art systems are vulnerable to them [48–50]. Due to their simplicity, implementing effective countermeasures that perform well against them should be a must for any facial recognition system.

- Information needed to perform the attack: image of the face of the subject to be impersonated.
- Generation and acquisition of the PAIs: there are plenty of options to obtain high-quality face images of the users to be impersonated, e.g., social networks, internet profiles, and hidden cameras. Then, those photographs can be printed or displayed on a screen in order to present them to the sensor of the FRS.
- Expected impact of the attack: most basic face recognition systems are vulnerable to this type of attack if specific countermeasures are not implemented. However, the literature offers a large number of approaches with good detection rates of printed photo attacks [44, 51].

9.2.1.2 Video Attacks

Similar to the case of photo attacks, video acquisition of people intended to be impersonated is also becoming increasingly easier with the growth of public video sharing sites and social networks, or even using a hidden camera. Another reason to use this type of attack is that it increases the probability of success by introducing liveness appearance to the displayed fake biometric sample [52, 53].

Once a video of the legitimate user is obtained, one attacker could play it in any device that reproduces video (smartphone, tablet, laptop, etc.) and then present it to the sensor/camera [54], (see Fig. 9.2). This type of attack is often referred to in the literature as replay attacks, a more sophisticated version of the simple photo attacks.

Replay attacks are more difficult to detect, compared to photo attacks, as not only the face texture and shape is emulated but also its dynamics, like eye-blinking, mouth and/or facial movements [26]. Due to their higher sophistication, it is reasonable to assume that systems that are vulnerable to photo attacks will perform even worse with respect to video attacks, and also that being resilient against photo attacks does not mean to be equally strong against video attacks [34]. Therefore, specific countermeasures need to be developed and implemented, e.g., an authentication protocol based on challenge-response [47].

- Information needed to perform the attack: video of the face of the subject to be impersonated.
- Generation and acquisition of the PAIs: similar to the case of photo attacks, obtaining face videos of the users to be impersonated is relatively easy thanks to the growth of video sharing platforms (YouTube, Twitch) and social networks (Face-

book, Instagram), and also using hidden cameras. The videos are then displayed on a screen in order to present them to the sensor of the FRS.
- Expected impact of the attack: like in the case of photo attacks most face recognition systems are inherently vulnerable to these attacks, and countermeasures based on challenge-response or in the appearance of the faces are normally implemented. With these countermeasures, classic video attacks have a low success rate.

9.2.1.3 Mask Attacks

In this type of attack, the PAI is a 3D mask of the user's face. The attacker builds a 3D reconstruction of the face and presents it to the sensor/camera. Mask attacks require more skills to be well executed than the previous attacks, and also access to extra information in order to construct a realistic mask of the genuine user [55, 56].

There are different types of masks depending on the complexity of the manufacturing process and the amount of data that is required. Some examples ordered from simpler to more complex are

- The simplest method is to print a 2D photograph of the user's face and then stick it to a deformable structure. Examples of this type of structures could be a t-shirt or a plastic bag. Finally, the attacker can put the bag on his face and present it to the biometric sensor [34]. This attack can mimic some deformable patterns of the human face, allowing to spoof some low-level 3D face recognition systems.
- Image reconstruction techniques can generate 3D models from 2 or more pictures of the genuine user's face, e.g., one frontal photo and a profile photo. Using these photographs, the attacker could be able to extrapolate a 3D reconstruction of the real face[1] (see Fig. 9.2). This method is unlikely to spoof top-level 3D face recognition systems, but it can be an easy and cheap option to spoof a high number of standard systems.
- A more sophisticated method consists in making directly a 3D capture of a genuine user's face [28, 56, 57] (see Fig. 9.3). This method entails a higher level of difficulty than the previous ones since a 3D acquisition can be done only with dedicated equipment and it is complex to obtain without the cooperation of the end-user. However, this is becoming more feasible and easier each day with the new generation of affordable 3D acquisition sensors [58].

When using any of the two last methods, the attacker would be able to build a 3D mask with the model he has computed. Even though the price of 3D printing devices is decreasing, 3D printers with sufficient quality and definition are still expensive. See references [56, 57] for examples of 3D-printed masks. There are some companies where such 3D face models may be obtained for a reasonable price.[2]

[1] https://3dthis.com, https://www.reallusion.com/character-creator/headshot.

[2] http://real-f.jp, https://shapify.me, and http://www.sculpteo.com.

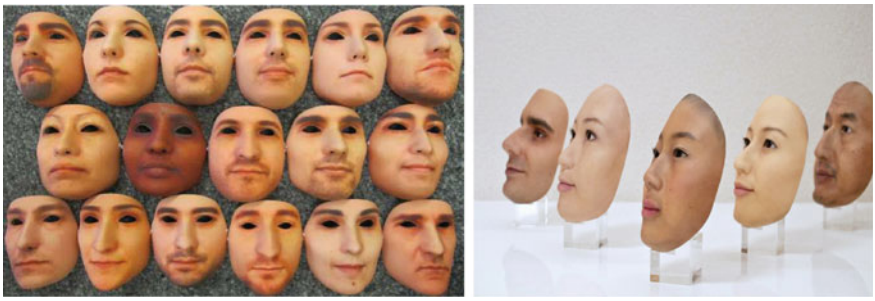

Fig. 9.3 Examples of 3D masks. (Left) The 17 hard-resin facial masks used to create the 3DMAD dataset, from [28]. (Right) Face Masks built by Real-F reproducing even the eyeballs and finest skin details

This type of attack may be more likely to succeed due to the high realism of the spoofs. As the complete structure of the face is imitated, it becomes difficult to find effective countermeasures. For example, the use of depth information becomes inefficient against this particular threat.

These attacks are far less common than the previous two categories because of the difficulties mentioned above to generate the spoofs. Despite the technical complexity, mask attacks have started to be systematically studied thanks to the acquisition of the first specific databases which include masks of different materials and sizes [28, 55–57, 59, 60].

- Information needed to perform the attack: 2D masks can be created using only one face image of the user to be impersonated. However, 3D realistic masks usually need 3 or more face images acquired from different angles.
- Generation and acquisition of the PAIs: compared to photo and video attacks it is more difficult to generate realistic 3D masks since the attacker needs images of high quality captured from different and complementary angles. Using the photographs, face masks can be ordered to third companies for a reasonable price.
- Expected impact of the attack: these attacks are more challenging than photo and video attacks because of the higher realism of the PAIs. However, they are less common due to the difficulty in generating the masks.

9.2.1.4 Other Attacks

There are other possibilities in order to circumvent a face recognition system, such as using DeepFake techniques, facial makeup, or modifications via plastic surgery.

Together with the recent availability of large-scale face databases, the progress of deep learning methods like Generative Adversarial Networks (GANs) [61] has led to the emergence of new realistic face manipulation techniques that can be used to spoof face recognition systems. The term Identity Swap (commonly known as

DeepFakes) includes the manipulation techniques consisting in replacing the face of one person in a video with the face of another person. User-friendly applications like FaceApp allow to create fake face images and videos without the need of any previous coding experience. Public information from social networks can be used to create realistic fake videos capable to spoof a FRS, e.g., by means of a replay attack. Recent examples of DeepFake video databases are Celeb-DF [27] and DFDC [62]. DeepFake techniques are evolving very fast, with their outputs becoming more and more realistic each day, so counter-measuring them is a very challenging problem [63, 64].

Works like [42] studied the impact of facial makeup in the accuracy of automatic face recognition systems. They focused their work on determining if facial makeup can affect the matching accuracy of a FRS. They acquired two different databases of females with and without makeup and they tested the accuracy of several face recognition systems when using those images. They concluded that the accuracy of the FRS is hugely impacted by the presence of facial makeup.

Nowadays, the technology advancements and the social acceptance have led to a higher presence of plastic surgery among the population. Therefore, the authors of [65, 66] focused their research on determining the level of affectation of face recognition accuracy when using images with presence of plastic surgery that modifies facial appearance. In [65] they reported a high reduction of face recognition accuracy (around a 30%) of several matching algorithms when comparing images with and without plastic surgery modifications.

- Information needed to perform the attack: in the case of DeepFake attacks, PAIs can be created only with a few photographs of the targeted subject. Makeup and surgery also need information about the face of the user to be impersonated.
- Generation and acquisition of the PAIs: similar to the case of the previous types of attacks, obtaining face images and videos of the users to be impersonated can be easy thanks to video sharing platforms and social networks. Then, the DeepFake videos can be displayed on a screen to present them to the camera of the FRS. Makeup-based attacks need of certain skills to achieve a high-quality makeup. Attacks based on surgery modifications are much harder to achieve since they need of highly qualified professionals and of some recovery time after the modifications.
- Expected impact of the attack: DeepFake attacks are more difficult to detect than other attacks and how to prevent them is a very active research area nowadays. Surgery attacks are also very difficult to detect since they are actually faces and not synthetic fakes. Makeup attacks, on the other hand, can be detected more easily using PAD techniques based on texture or color, like in the case of photo and video attacks.

9.3 Presentation Attack Detection

Face recognition systems are designed to differentiate between genuine users, not to determine if the biometric sample presented to the sensor is legitimate or a fake. A presentation attack detection method is usually accepted to be any technique that is able to automatically distinguish between legitimate biometric characteristics presented to the sensor and artificially produced PAIs.

Presentation attack detection can be done in four different ways [16]: (i) with dedicated hardware to detect an evidence of liveness, which is not always possible to deploy, (ii) with a challenge-response method where a presentation attack can be detected by requesting the user to interact with the system in a specific way, (iii) employing recognition algorithms intrinsically resilient against attacks, and (iv) with software that uses already available sensors to detect any pattern characteristic of live traits. Figure 9.4 shows how PAD methods are organized according to this proposed taxonomy.

- **Hardware-based:** PAD approaches based on dedicated hardware usually take benefit of special sensors like Near Infrared (NIR) cameras [37], thermal sensors [67], Light Field Cameras (LFC) [68], multi-spectral sensors [69], and 3D cameras [70]. Using the unique properties of the different types of dedicated hardware, the biological and physical characteristics of legitimate faces can be measured and distinguished from PAIs more easily, e.g., processing temperature information with thermal cameras [71] and estimating the 3D volume of the artifacts thanks to 3D acquisition sensors [70]. However, these approaches are not popular even though they tend to achieve high presentation detection rates, because in most systems the required hardware is expensive and not broadly available.
- **Challenge-Response:** These PAD methods present a challenge to the user, i.e., completing a predefined task, or expose them to a stimulus in order to record their voluntary or involuntary response. Then that response is analyzed to decide if the access attempt comes from a legitimate user or from an attacker. An example of this approach can be found in [72], where the authors studied the involuntary eye response of users exposed to a visual stimulus. Other examples are [47] where the authors requested the users to make specific movements with their eyes and [73] where the users were indicated to say some predefined words. Challenge-response

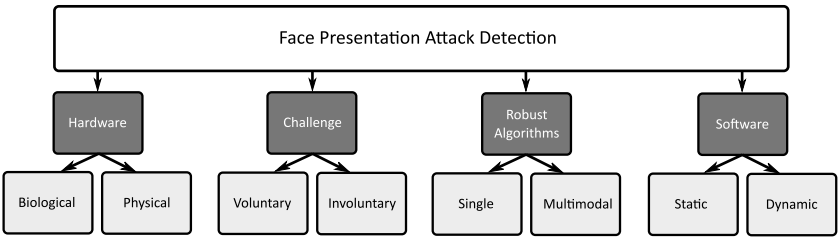

Fig. 9.4 Taxonomy of face presentation attack detection methods

methods can be effective against many presentation attacks but they usually require more time and cooperation from users' side, something that is not always possible or desirable.
- **Robust algorithms:** Existing face recognition systems can be designed or trained to learn how to distinguish between legitimate faces and PAIs, making them inherently robust to some types of presentation attacks. However, developing face recognition algorithms intrinsically robust against presentation attacks is not straightforward and the most common approach consists in relying on multimodal biometrics to increment the security level thanks to the information coming from the other biometric modalities.

The limitations of these three types of PAD methods, together with the easiness of deploying software-based PAD methods, have made most of the literature on face Presentation Attack Methods (PAD) to be focused on running software-based PAD algorithms over already deployed hardware. This is why in the next part of the chapter we focus on describing software-based PAD and the different categories that compose this type of approach.

9.3.1 Software-Based Face PAD

Software-based PAD methods are convenient in most of the cases since they allow to upgrade the countermeasures in existing systems without needing new pieces of hardware and permitting authentication to be done in real time without extra user interaction. Table 9.1 shows a selection of relevant PAD works based on software techniques, including information about the type of images they use, the databases in which they are evaluated, and the types of features they analyze. The table also illustrates the current dominance of deep learning among PAD methods, since like in many other research areas, during the last years most state-of-the-art face PAD works have changed from methods based on hand-crafted features to deep learning approaches based on architectures like Convolutional Neural Networks and Generative Adversarial Networks.

Regardless of whether they belong to one category (hand-crafted) or the other (deep learning), software-based PAD methods can be divided into two main categories depending on whether they take into account temporal information or not: static and dynamic analysis.

9.3.1.1 Static Analysis

This subsection refers to the development of techniques that analyze static features like the facial texture to discover unnatural characteristics that may be related to presentation attacks.

Table 9.1 Selection of relevant works in software-based face PAD

Method	Year	Type of images	Database used	Type of features
[74]	2009	Visible and IR photo	Private	Color (reflectance)—Hand Crafted
[46]	2011	RGB video	PRINT-ATTACK	Face-background motion—Hand Crafted
[26]	2012	RGB video	REPLAY-ATTACK	Texture based—Hand Crafted
[75]	2013	RGB photo and video	NUAA PI, PRINT-ATTACK and CASIA FAS	Texture based—Hand Crafted
[51]	2013	RGB photo and video	PRINT-ATTACK and REPLAY ATTACK	Texture based—Hand Crafted
[44]	2013	RGB video	PHOTO-ATTACK	Motion correlation analysis—Hand Crafted
[76]	2014	RGB video	REPLAY-ATTACK	Image Quality based—Hand Crafted
[77]	2015	RGB video	Private	Color (challenge reflections)—Hand Crafted
[78]	2016	RGB video	3DMAD and private	rPPG (color based)—Hand Crafted
[79]	2017	RGB video	OULU-NPU	Texture based—Hand Crafted
[37]	2018	RGB and NIR video	3DMAD and private	rPPG (color based)—Hand Crafted
[35]	2019	RGB, Depth and NIR video	WMCA	Fine-tuned face recog. features—Deep Learning
[64]	2020	RGB video	Celeb-DF v2 and DFDC	rPPG (color based)—Deep Learning
[80]	2021	RGB, Depth, Thermal, and NIR video	WMCA, MLFP, and SiW-M	Spoof-specific info.—Deep Learning
[81]	2021	RGB video	3DMAD and HKBU-MARsV2	rPPG (color based)—Deep Learning

The key idea of the texture-based approach is to learn and detect the structure of facial micro-textures that characterize real faces but not fake ones. Micro-texture analysis has been effectively used in detecting photo attacks from single face images: extraction of texture descriptions such as Local Binary Patterns (LBP) [26] or Gray-Level Co-occurrence Matrices (GLCM) followed by a learning stage to perform discrimination between textures.

For example, the recapturing process by a potential attacker, the printing of an image to create a spoof, usually introduces quality degradation in the sample, making it possible to distinguish between a genuine access attempt and an attack, by analyzing their textures [76].

The major drawback of texture-based presentation attack detection is that high-resolution images are required in order to extract the fine details from the faces that are needed for discriminating genuine faces from presentation attacks. These countermeasures will not work properly with bad illumination conditions that make the captured images to have bad quality in general.

Most of the time, the differences between genuine faces and artificial materials can be seen in images acquired in the visual spectrum with or without a preprocessing stage. However, sometimes a translation to a more proper feature space [82], or working with images from outside the visible spectrum [83] is needed in order to distinguish between real faces and spoof-attack images.

Additionally to the texture, there are other properties of the human face and skin that can be exploited to differentiate between real and fake samples. Some of these properties are: absorption, reflection, scattering, and refraction [74].

This type of approaches may be useful to detect photo attacks, video attacks, and also mask attacks, since all kinds of spoofs may present texture or optical properties different than real faces.

In recent years, to improve the accuracy of traditional static face PAD methods the researchers have been focused on applying the power of deep learning to face PAD mainly using transfer-learning from face recognition. This technique makes possible to adapt facial features learned for face recognition to face presentation attack detection without the need of a huge amount of labeled data. This is the case of [35] where the authors transfer facial features learned for face recognition and used them for detecting presentation attacks. Finally, to increase the generalization ability of their method to unseen attacks, they fused the decisions of different models trained with distinct types of attacks.

However, even though deep learning methods have shown to be really accurate when evaluated in intra-database scenarios, their performance usually drops significantly when they are tested under inter-database scenarios. Deep learning models are capable of learning directly from data, but they are normally overfitted to the training databases, causing poor generalization of the resulting models when facing data from other sources. To avoid this, the most recent works in the literature face this problem by implementing domain generalization techniques. For example, the authors of [80] introduced a novel loss function to force their model to learn a compact embedding for genuine faces while being far from the embeddings of the different presentation attacks.

9.3.1.2 Dynamic Analysis

These techniques have the target of distinguishing presentation attacks from genuine access attempts based on the analysis of motion. The analysis may consist in detecting any physiological sign of life, for example: pulse [84], eye-blinking [85], facial expression changes [22], or mouth movements. This objective is achieved using knowledge of the human anatomy and physiology.

As stated in Sect. 9.2, photo attacks are not able to reproduce all signs of life because of their static nature. However, video attacks and mask attacks can emulate blinking, mouth movements, etc. Related to these types of presentation attacks, it can be assumed that the movement of the PAIs, differs from the movement of real human faces which are complex nonrigid 3D objects with deformations.

One simple approximation to this type of countermeasures consists in trying to find correlations between the movement of the face and the movement of the background with respect to the camera [44, 54]. If the fake face presented contains also a piece of fake background, the correlation between the movement of both regions should be high. This could be the case of a replay attack, in which the face is shown on the screen of some device. This correlation in the movements allows to evaluate the degree of synchronization within the scene during a defined period of time. If there is no movement, as in the case of a fixed support attack, or too much movement, as in a hand-based attack, the input data is likely to come from a presentation attack. Genuine authentication will usually have uncorrelated movement between the face and the background, since user's head generally moves independently from the background.

Another example of this type of countermeasure is [53] where the authors propose a method for detecting face presentation attacks based on properties of the scenario and the facial surfaces such as albedo, depth, and reflectance.

A high number of the software-based PAD techniques are based on liveness detection without needing any special help of the user. These presentation attack detection techniques aim to detect some physiological signs of life such as eye-blinking [75, 85, 86], facial expression changes [22], and mouth movements.

Other works like [51] provide more evidence of liveness using Eulerian video magnification [87] applying it to enhance small changes in face regions, that often go unnoticed. Some changes that are amplified thanks to this technique are, for example, small color and motion changes on the face caused by the human blood flow, by finding peaks in the frequency domain that correspond to the human heartbeat rate. Works like [37, 64, 81] use remote photoplethysmography for liveness detection, and more specifically 3D mask PAD, without relying on the appearance features of the spoof like the texture, shape, etc.

As mentioned above, motion analysis approaches usually require some level of motion between different head parts or between the head and the background. Sometimes this can be achieved through user cooperation [77]. Therefore, some of these techniques can only be used in scenarios without time requirements as they may need time for analyzing a piece of video and/or for recording the user's response to a command. Due to the nature of these approaches, some videos and well-performed mask attacks may deceive the countermeasures.

9.4 Face Presentation Attacks Databases

In this section, we overview some publicly available databases for research in face PAD. The information contained in these datasets can be used for the development and evaluation of new face PAD techniques against presentation attacks.

As it has been mentioned in the past sections, with the recent spread of biometric applications, the threat of presentation attacks has grown, and the biometric community is starting to acquire large and comprehensive databases to make recognition systems more resilient against presentation attacks.

International competitions have played a key role to promote the development of PAD measures. These competitions include the recent LivDet-Face 2021 [36], the CelebA-Spoof Challenge 2020 [27], the ChaLearn Face Antispoofing Attack Detection Challenge 2019 [88], the Multi-modal Face Anti-spoofing (Presentation Attack Detection) Challenge 2019 [89], the Competition on Generalized Face Presentation Attack Detection in Mobile Authentication Scenarios 2017 [33], and the 2011 and 2013 2D Face Anti-Spoofing contests [31, 32].

Despite the increasing interest of the community in studying the vulnerabilities of face recognition systems, the availability of PAD databases is still scarce. The acquisition of new datasets is highly difficult because of two main reasons:

- Technical aspects: the acquisition of presentation attack data offers additional challenges to the usual difficulties encountered in the acquisition of standard biometric databases [90] in order to correctly capture similar fake data than the present in real attacks (e.g., generation of multiple types of PAIs).
- Legal aspects: as in the face recognition field in general, data protection limits the distribution or sharing of biometric databases among research groups. These legal restrictions have forced most laboratories or companies working in the field of presentation attacks to acquire their own datasets usually small and limited.

In the area of face recognition PAD, we can find the following public databases (ordered chronologically following their publication date):

- The NUAA Photo Imposter Database (NUAA PI DB) [25] was one of the first efforts to generate a large public face PAD dataset. It contains images of real-access attempts and print attacks of 15 users. The images contain frontal faces with a neutral expression captured using a webcam. Users were also told to avoid eye blinks. The attacks are performed using printed photographs on photographic paper. Examples from this database can be seen in Fig. 9.5. The NUAA PI DB is property of the Nanjing University of Aeronautics and Astronautics, and it can be obtained at http://parnec.nuaa.edu.cn/_upload/tpl/02/db/731/template731/pages/xtan/NUAAImposterDB_download.html.
- The PRINT-ATTACK DB [46] represents another step in the evolution of face PAD databases, both in terms of the size (50 different users were captured) and of the types of data acquired (it contains video sequences instead of still images). It only considers the case of photo attacks. It consists of 200 videos of real accesses and

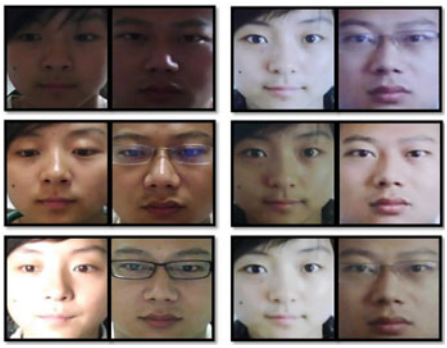

Fig. 9.5 Samples from the NUAA Photo Imposter Database [25]. Samples from two different users are shown. Each row corresponds to one different session. In each row, the left pair are from a live human and the right pair from a photo fake. Images have been taken from [25]

200 videos of print attack attempts from 50 different users. Videos were recorded under two different backgrounds and illumination conditions. Attacks were carried out with hard copies of high-resolution photographs of the 50 users, printed on plain A4 paper. The PRINT-ATTACK DB is property of the Idiap Research Institute, and it can be obtained at https://www.idiap.ch/en/dataset/printattack.

- The REPLAY-ATTACK database citeChingovskaspsBIOSIGsps2012 is an extension of the PRINT-ATTACK database. It contains short videos of both real-access and presentation attack attempts of 50 different subjects. The attack attempts present in the database are 1300 photo and video attacks using mobile phones and tablets under different lighting conditions. The attack attempts are also distinguished depending on how the attack device is held: hand-based and fixed-support. Examples from this database can be seen in Fig. 9.6. It can be obtained at https://www.idiap.ch/en/dataset/replayattack/.
- The 3D MASK-ATTACK DB (3DMAD) [28], as its name indicates, contains information related to mask attacks. As described above, all previous databases contain attacks performed with 2D spoofing artifacts (i.e., photo or video) that are very rarely effective against systems capturing 3D face data. It contains access attempts of 17 different users. The attacks were performed with real-size 3D masks manufactured by ThatsMyFace.com.[3] For each access attempt a video was captured using the Microsoft Kinect for Xbox 360, that provides RGB data and also depth information. That allows to evaluate both 2D and 3D PAD techniques, and also their fusion [57]. Example masks from this database can be seen in Fig. 9.3. 3DMAD is property of the Idiap Research Institute, and it can be obtained at https://www.idiap.ch/dataset/3dmad.
- The OULU-NPU DB [79] contains information of presentation attacks acquired with mobile devices. Nowadays mobile authentication is one of the most relevant scenarios due to the wide spread of the use of smartphones. However, in most datasets the images are acquired in constrained conditions. This type of data may present motion, blur, and changing illumination conditions, backgrounds and head poses. The database consists of 5, 940 videos of 55 subjects recorded in three dis-

[3] http://www.thatsmyface.com/.

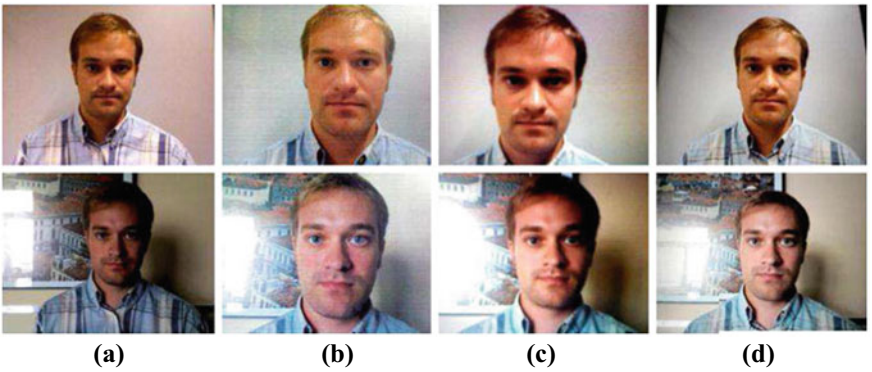

Fig. 9.6 Examples of real and fake samples from the REPLAY-ATTACK DB [26]**.** The images come from videos acquired in two illumination and background scenarios (controlled and adverse). The first row belongs to the controlled scenario while the second row represents the adverse conditions. **a** Shows real samples, **b** shows samples of a printed photo attack, **c** corresponds to a LCD photo attack, and **d** to a high-definition photo attack

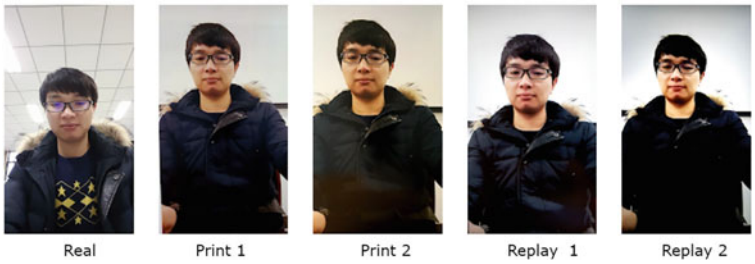

Fig. 9.7 Examples of bona-fide and attack samples from OULU-NPU DB [79]**.** The images come from videos acquired with mobile devices. The figure shows a legitimate sample, two examples of print attacks, and other two examples of replay attacks. Image extracted from https://sites.google.com/site/oulunpudatabase

tinct illumination conditions, with 6 different smartphone models. The resolution of all videos is 1920 × 1080 and it comprehends print and video-replay attacks. The OULU-NPU DB is property of the University of Oulu and it has been used in the IJCB 2017 Competition on Generalized Face Presentation Attack Detection [33]. Examples from this database can be seen in Fig. 9.7 and it can be obtained at https://sites.google.com/site/oulunpudatabase/.

- The Custom Silicone Mask Attack Dataset (CSMAD) [56] (collected at the Idiap Research Institute) contains 3D mask presentation attacks. It is comprised of face data from 14 subjects, from which 6 subjects have been selected to construct realistic silicone masks (made by Nimba Creations Ltd.). The database contains 87 bona-fide videos and 159 attack videos captured under four different lighting conditions. CSMAD is composed of RGB, Depth, NIR, and thermal videos of

10 seconds of duration. The database can be obtained at https://www.idiap.ch/en/dataset/csmad.

- The Spoof in the Wild (SiW) Database [91] provides bona-fide and presentation attacks from 165 different subjects. For each of those subjects, the database contains 8 live and up to 20 spoof videos recorded at 30 fps and 1920 × 1080 pixels of resolution, making a total of 4, 478 video sequences. The database was acquired in order to have several types of distances to faces, poses, illumination conditions, and facial expressions. The collection of PAIs comprehends paper print photo attacks and video-replay attacks.
- The Wide Multi-Channel Presentation Attack Database (WMCA) [35] consists of video recordings of 10 seconds for both bona-fide attempts and presentation attacks. The database is composed of RGB, Depth, NIR, and thermal videos of 72 different subjects, with 7 sessions for each subject. WCMA contains 2D and 3D presentation attacks including print, replay, and paper and silicone mask attacks. The total number of videos in the database is 1,679 (1,332 are attacks).
- The CelebA-Spoof Database [27] is a large-scale face anti-spoofing dataset with 625, 537 images from 10, 177 different subjects. The database includes labels for 43 attributes related to the face, the illumination conditions, the environment, and the spoof types. The spoof images were captured on 2 different environments and under 4 illumination conditions using 10 different acquisition devices. CelebA-Spoof contains 10 different attack types, e.g., print attacks, replay attacks, and 3D masks. The database can be obtained at https://github.com/Davidzhangyuanhan/CelebA-Spoof.
- The High-Quality Wide Multi-Channel Attack Database (HQ-WMCA) [92] is an extension of the WMCA database. However, they differ in several important aspects like frame rate and resolution and the use of a new sensor for the ShortWave InfraRed spectrum (SWIR) during the acquisition. Additionally, it contains a wider range of attacks than the previous database, incorporating obfuscation attacks, where the attacker tries to hide its identity. In the database, there are 555 bona-fide presentations from 51 participants and the remaining 2, 349 are presentation attacks. RGB, NIR, SWIR, thermal, and depth information was acquired, with each recording containing data in 14 different bands, including 4 NIR and 7 SWIR wavelengths. The PAIs used can be grouped into ten different categories ranging from glasses to flexible masks (including makeup).
- The LiveDet Database [36] is a dataset built as a combination of data from two of the organizers of the Face Liveness Detection Competition (LivDet-Face 2021), i.e., Clarkson University (CU) and Idiap Research Institute. The final database contains data from 48 subjects, with a total of 724 images and 814 videos (of 6 seconds) acquired using 5 different sensors including reflex cameras and mobile devices. 8 different presentation artifacts were used for the images and 9 for the videos, comprehending paper photographs, photographs shown from digital screens (e.g., a laptop), paper masks, 3D silicone masks, and video replays. Additional details of LiveDet can be found at https://face2021.livdet.org/.

Finally, we include the description of two of the most challenging DeepFake databases up to date [93, 94], i.e., Celeb-DF v2 and DFDC. The videos in these databases contain DeepFakes with a large range of variations in face sizes, illumination, environments, pose variations, etc. DeepFake videos can be used, for example, to create a video with the face of a user and use it for a replay attack against a FRS.

- Celeb-DF v2 [27] is a database that consists of 590 legitimate videos extracted from YouTube, corresponding to celebrities of different gender, age, and ethnic group. Regarding fake videos, a total of 5,639 videos were created swapping faces using DeepFake technology. The average length of the face videos is around 13 seconds (at 30 fps).
- DFDC Preview Database [95] is one of the latest public databases, released by Facebook in collaboration with other institutions like Amazon, Microsoft, and the MIT. The DFDC Preview dataset consists of 1,131 legitimate videos from 66 different actors, ensuring realistic variability in gender, skin tone, and age. A total of 4,119 videos were created using two different DeepFake generation methods by swapping subjects with similar appearances.

In Table 9.2, we show a comparison of the most relevant features of all the databases described in this section.

9.5 Integration with Face Recognition Systems

In order to create a face recognition system resistant to presentation attacks, the proper PAD techniques have to be selected. After that, the integration of the PAD countermeasures with the FRS can be done at different levels, namely, score-level or decision-level fusion [96, 97].

The first possibility consists in using score level fusion as shown in Fig. 9.8. This is a popular approach due to its simplicity and the good results given in fusion of multimodal biometric systems [98–100]. In this case, the biometric data enter at the same time to both the face recognition system and the PAD system, and each one computes its own scores. Then the scores from each system are combined into a new final score that is used to determine if the sample comes from a genuine user or not. The main advantage of this approach is its speed, as both modules, i.e., the PAD and face recognition modules, perform their operations at the same time. This fact can be exploited in systems with good parallel computation specifications, such as those with multicore/multithread processors.

Another common way to combine PAD and face recognition systems is a serial scheme, as in Fig. 9.9, in which the PAD system makes its decision first, and only if the samples are determined to come from a living person, then they are processed by the face recognition system. Thanks to this decision-level fusion, the FRS will search for the identity that corresponds to the biometric sample knowing previously that the sample does not come from a presentation attack. Different from the parallel

Table 9.2 Features of the main public databases for research in face PAD. Comparison of the most relevant features of each of the databases described in this chapter

Database	Users # (real/fakes)	Samples # (real/fakes)	Attack types	Support	Attack illumination
NUAA PI [25]	15/15	5,105/7,509	Photo	Held	Uncont.
REPLAY-ATTACK [26, 44, 46]	50/50	200/1,000	Photo and Replay	Held and Fixed	Cont. and Uncont.
3DMAD [28]	17/17	170/85	Mask	Held	Cont.
OULU-NPU [79]	55/55	1,980/3,960	Photo and Replay	Mobile	Uncont.
CSMAD [56]	14/6	87/159	Photo and Replay	Held and Fixed	Cont.
SiW [91]	165/165	1,320/3,158	Photo and Replay	Held	Uncont.
WMCA [35]	72/72	347/1,332	Photo, Replay, and Mask	Held	Uncont.
CelebA-Spoof [27]	10,177/10,177	202,599/422,938	Photo, Replay, and Mask	Held	Uncont.
HQ-WMCA [92]	51/51	555/2,349	Photo, Replay, Mask, Makeup, others.	Held	Uncont.
LiveDet [36]	48/48	125/689	Photo, Replay, and Mask	Held	Uncont.
CelebDF-v2 [27]	59/59	590/5,639	DeepFakes	–	Uncont.
DFDC Preview [95]	66/66	1,131/4,119	DeepFakes	–	Uncont.

Containing also PHOTO-ATTACK DB and PRINT-ATTACK DB

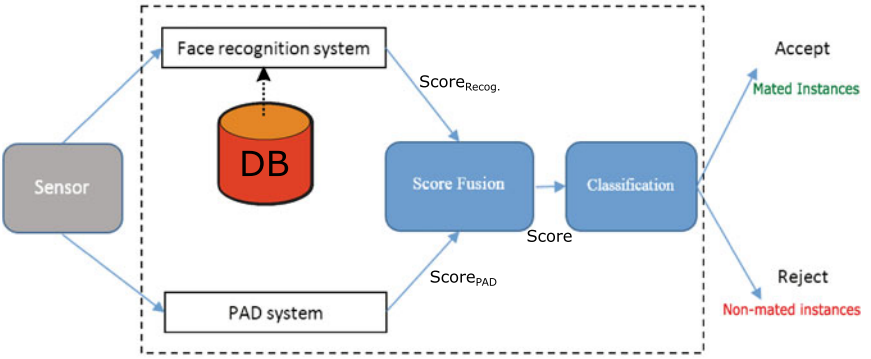

Fig. 9.8 Scheme of a parallel score-level fusion between a PAD and a face recognition system. In this type of scheme, the input biometric data is sent at the same time to both the face recognition system and the PAD system, and each one generates a independent score, then the two scores are fused to take one unique decision

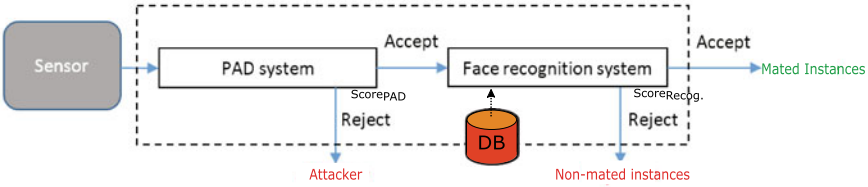

Fig. 9.9 Scheme of a serial fusion between a PAD and a face recognition system. In this type of scheme the PAD system makes its decision first, and only if the samples are determined to come from a living person, then they are processed by the face recognition system

approach, in the serial scheme the average time for an access attempt will be longer due to the consecutive delays of the PAD and the face recognition modules. However, this approach avoids extra work to the face recognition system in the case of a PAD attack, since it should be detected in an early stage.

9.6 Conclusion and Look Ahead on Face PAD

Face recognition systems are increasingly being deployed in a diversity of scenarios and applications. Due to this widespread use, they have to withstand a high variety of attacks. Among all these threats, one with high impact are presentation attacks.

In this chapter, an introduction of the strengths and vulnerabilities of face as a biometric characteristic has been presented, including key resources and advances in the field in the last few years. We have described the main presentation attacks, differentiating between multiple approaches, the corresponding PAD countermeasures, and the public databases that can be used to evaluate new protection techniques. The weak points of the existing countermeasures have been stated, and also some possible future directions to deal with those weaknesses have been discussed.

Due to the nature of face recognition systems, without the correct PAD countermeasures, most of the state-of-the-art systems are vulnerable to attacks since they do not integrate any module to discriminate between legitimate and fake samples. Usually, PAD techniques are developed to fight against one concrete type of attack (e.g., printed photos), retrieved from a specific dataset. The countermeasures are thus designed to achieve high presentation attack detection against that particular spoof technique. However, when testing these same techniques against other types of PAIs (e.g., video-replay), usually the system is unable to efficiently detect them. There is one important lesson to be learned from this fact: there is not a superior PAD technique that outperforms all the others in all conditions; so knowing which technique to use against each type of attack is a key element. It would be interesting to use different countermeasures that have proved to be effective against particular types of PAIs, in order to develop fusion schemes that combine their results, achieving that way a high performance against a variety of presentation attacks data [16, 98, 99]. This

problem becomes more relevant in the case of DeepFakes, a term that includes those methods capable of generating images and videos with very realistic face spoofs using deep learning methods and few input data. When dealing with DeepFakes, cross-data generalization is one of the main open problems at present. The majority of the most accurate DeepFake detection solutions nowadays are highly overfitted to the techniques present in their training databases, therefore, their detection accuracy is usually poor when facing fakes created using other techniques unseen during training.

In addition, as technology progresses constantly, new hardware devices and software techniques continue to appear. From the detection point of view, it is also important to keep track of this quick technological progress in order to use it to develop more efficient presentation attack detection techniques. For example, using the power of deep learning and some of its associated techniques like transfer-learning has shown to improve the accuracy of PAD methods in the recent years [35]. Additionally, focusing the research on the biological nature of biometric characteristics (e.g., thermogram, blood flow, etc.) should be considered [64, 78], as the standard techniques based on texture and movement seem to be inefficient against some PAIs.

Additionally, it is of the utmost importance to collect new databases with new scenarios in order to develop more effective PAD methods. Otherwise, it will be difficult to grant an acceptable level of security of face recognition systems. However, it is especially challenging to recreate realistic attacking conditions in a laboratory evaluation. Under controlled conditions, systems are tested against a restricted number of typical PAIs. These restrictions make it unfeasible to collect a database with all the different fake spoofs that may be found in the real world.

To conclude this introductory chapter, it could be said that even though a great amount of work has been done to fight face presentation attacks, there are still big challenges to be addressed in this topic, due to the evolving nature of the attacks, and the critical applications in which these systems are deployed in the real world.

Acknowledgements This work was mostly done (2nd Edition of the book) in the context of the TABULA RASA and BEAT projects funded under the 7th Framework Programme of EU. The 3rd Edition update has been made in the context of EU H2020 projects PRIMA and TRESPASS-ETN. This work was also partially supported by the Spanish project BIBECA (RTI2018-101248-B-I00 MINECO/FEDER).

References

1. Galbally J, Ferrara P, Haraksim R, Psyllos A, Beslay L (2019) Study on face identification technology for its implementation in the Schengen information system. Joint Research Centre, Ispra, Italy, Rep. JRC-34751
2. Tome P, Fierrez J, Vera-Rodriguez R, Nixon MS (2014) Soft biometrics and their application in person recognition at a distance. IEEE Trans Inf Forensics Secur 9(3):464–475

3. Alonso-Fernandez F, Farrugia RA, Fierrez J, Bigun J (2019) Super-resolution for selfie biometrics: introduction and application to face and iris. In: Selfie biometrics. Springer, pp 105–128
4. Tome P, Vera-Rodriguez R, Fierrez J, Ortega-Garcia J (2015) Facial soft biometric features for forensic face recognition. Forensic Sci Int 257:271–284
5. Hernandez-Ortega J, Daza R, Morales A, Fierrez J, Ortega-Garcia J (2020) edBB: biometrics and behavior for assessing remote education. In: AAAI workshop on artificial intelligence for education (AI4EDU)
6. Turk MA, Pentland AP (1991) Face recognition using eigenfaces. In: Computer society conference on computer vision and pattern recognition (CVPR), pp 586–591
7. International biometric group and others: biometrics market and industry report 2009-2014 (2007)
8. Richardson R (2021). https://www.gmfus.org/news/facial-recognition-public-sector-policy-landscape
9. Gipp B, Beel J, Rössling I (2007) ePassport: the world's new electronic passport. A Report about the ePassport's Benefits, Risks and it's Security. CreateSpace
10. Garcia C (2004) Utilización de la firma electrónica en la Administración española iv: Identidad y firma digital. El DNI electrónico, Administración electrónica y procedimiento administrativo
11. Jain AK, Li SZ (2011) Handbook of face recognition. Springer
12. Tistarelli M, Champod C (2017) Handbook of biometrics for forensic science. Springer
13. Zhao J, Cheng Y, Xu Y, Xiong L, Li J, Zhao F, Jayashree K, Pranata S, Shen S, Xing J et al (2018) Towards pose invariant face recognition in the wild. In: IEEE conference on computer vision and pattern recognition (CVPR), pp 2207–2216
14. Li P, Prieto L, Mery D, Flynn PJ (2019) On low-resolution face recognition in the wild: comparisons and new techniques. IEEE Trans Inf Forensics Secur 14(8):2000–2012
15. Gonzalez-Sosa E, Fierrez J, Vera-Rodriguez R, Alonso-Fernandez F (2018) Facial soft biometrics for recognition in the wild: recent works, annotation and COTS evaluation. IEEE Trans Inf Forensics Secur 13(8):2001–2014
16. Hadid A, Evans N, Marcel S, Fierrez J (2015) Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. IEEE Signal Process Mag 32(5):20–30
17. Li L, Correia PL, Hadid A (2018) Face recognition under spoofing attacks: countermeasures and research directions. IET Biom 7(1):3–14
18. Galbally J, Fierrez J, Ortega-Garcia J (2007) Vulnerabilities in biometric systems: attacks and recent advances in liveness detection. In: Proceedings of Spanish workshop on biometrics, (SWB)
19. Galbally J, Marcel S, Fierrez J (2014) Biometric antispoofing methods: a survey in face recognition. IEEE Access 2:1530–1552
20. Gomez-Barrero M, Galbally J, Fierrez J, Ortega-Garcia J (2013) Multimodal biometric fusion: a study on vulnerabilities to indirect attacks. In: Iberoamerican congress on pattern recognition. Springer, pp 358–365
21. Martinez-Diaz M, Fierrez J, Galbally J, Ortega-Garcia J (2011) An evaluation of indirect attacks and countermeasures in fingerprint verification systems. Pattern Recognit Lett 32:1643–1651
22. Pena A, Serna I, Morales A, Fierrez J, Lapedriza A (2021) Facial expressions as a vulnerability in face recognition. In: IEEE international conference on image processing (ICIP), pp 2988–2992
23. Newman LH (2016). https://www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/
24. Goodin D (2008) Get your german interior minister's fingerprint here. The Register 30
25. Tan X, Li Y, Liu J, Jiang L (2010) Face liveness detection from a single image with sparse low rank bilinear discriminative model. Computer Vision–ECCV, pp 504–517
26. Chingovska I, Anjos A, Marcel S (2012) On the effectiveness of local binary patterns in face anti-spoofing. In: IEEE BIOSIG

27. Li Y, Yang X, Sun P, Qi H, Lyu S (2020) Celeb-DF: a large-scale challenging dataset for DeepFake forensics. In: IEEE/CVF conference on computer vision and pattern recognition (CVPR)
28. Erdogmus N, Marcel S (2014) Spoofing face recognition with 3D masks. IEEE Trans Inf Forensics Secur 9(7):1084–1097
29. Proceedings IEEE International Conference on Acoustics Speech Signal Process (ICASSP) (2017)
30. Proceedings of IEEE/IAPR international joint conference on biometrics (IJCB) (2017)
31. Chakka MM, Anjos A, Marcel S, Tronci R, Muntoni D, Fadda G, Pili M, Sirena N, Murgia G, Ristori M, Roli F, Yan J, Yi D, Lei Z, Zhang Z, Li SZ, Schwartz WR, Rocha A, Pedrini H, Lorenzo-Navarro J, Castrillón-Santana M, Määttä J, Hadid A, Pietikäinen M (2011) Competition on counter measures to 2-D facial spoofing attacks. In: IEEE international joint conference on biometrics (IJCB)
32. Chingovska I, Yang J, Lei Z, Yi D, Li SZ, Kahm O, Glaser C, Damer N, Kuijper A, Nouak A et al (2013) The 2nd competition on counter measures to 2D face spoofing attacks. In: International conference on biometrics (ICB)
33. Boulkenafet Z, Komulainen J, Akhtar Z, Benlamoudi A, Samai D, Bekhouche S, Ouafi A, Dornaika F, Taleb-Ahmed A, Qin L et al (2017) A competition on generalized software-based face presentation attack detection in mobile scenarios. In: International joint conference on biometrics (IJCB), pp 688–696
34. Zhang Z, Yan J, Liu S, Lei Z, Yi D, Li SZ (2012) A face antispoofing database with diverse attacks. In: International conference on biometrics (ICB), pp 26–31
35. George A, Mostaani Z, Geissenbuhler D, Nikisins O, Anjos A, Marcel S (2019) Biometric face presentation attack detection with multi-channel convolutional neural network. IEEE Trans Inf Forensics Secur 15:42–55
36. Purnapatra S, Smalt N, Bahmani K, Das P, Yambay D, Mohammadi A, George A, Bourlai T, Marcel S, Schuckers S et al (2021) Face liveness detection competition (LivDet-Face)-2021. In: IEEE international joint conference on biometrics (IJCB)
37. Hernandez-Ortega J, Fierrez J, Morales A, Tome P (2018) Time analysis of pulse-based face anti-spoofing in visible and NIR. In: IEEE CVPR computer society workshop on biometrics
38. ISO: information technology security techniques security evaluation of biometrics, ISO/IEC Standard ISO/IEC 19792:2009, 2009. International Organization for Standardization (2009). https://www.iso.org/standard/51521.html
39. ISO: Information technology – Biometric presentation attack detection – Part 1: Framework. International Organization for Standardization (2016). https://www.iso.org/standard/53227.html
40. Kim J, Choi H, Lee W (2011) Spoof detection method for touchless fingerprint acquisition apparatus. Korea Pat 1(054):314
41. Raguin DH (2020) System for presentation attack detection in an iris or face scanner. US Patent 10,817,722
42. Dantcheva A, Chen C, Ross A (2012) Can facial cosmetics affect the matching accuracy of face recognition systems? In: IEEE international conference on biometrics: theory, applications and systems (BTAS). IEEE, pp 391–398
43. Chen C, Dantcheva A, Swearingen T, Ross A (2017) Spoofing faces using makeup: an investigative study. In: IEEE international conference on identity, security and behavior analysis (ISBA)
44. Anjos A, Chakka MM, Marcel S (2013) Motion-based counter-measures to photo attacks in face recognition. IET Biom 3(3):147–158
45. Peng F, Qin L, Long M (2018) Face presentation attack detection using guided scale texture. Multimed Tools Appl 77(7):8883–8909
46. Anjos A, Marcel S (2011) Counter-measures to photo attacks in face recognition: a public database and a baseline. In: International joint conference on biometrics (IJCB)
47. Shen M, Wei Y, Liao Z, Zhu L (2021) IriTrack: face presentation attack detection using iris tracking. In: ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 5(2)

48. Nguyen D, Bui Q (2009) Your face is NOT your password. BlackHat DC
49. Scherhag U, Raghavendra R, Raja KB, Gomez-Barrero M, Rathgeb C, Busch C (2017) On the vulnerability of face recognition systems towards morphed face attacks. In: IEEE international workshop on biometrics and forensics (IWBF)
50. Ramachandra R, Venkatesh S, Raja KB, Bhattacharjee S, Wasnik P, Marcel S, Busch C (2019) Custom silicone face masks: Vulnerability of commercial face recognition systems & presentation attack detection. In: IEEE international workshop on biometrics and forensics (IWBF)
51. Bharadwaj S, Dhamecha TI, Vatsa M, Singh R (2013) Computationally efficient face spoofing detection with motion magnification. In: Proceedings of the ieee conference on computer vision and pattern recognition workshops, pp 105–110
52. da Silva Pinto A, Pedrini H, Schwartz W, Rocha A (2012) Video-based face spoofing detection through visual rhythm analysis. In: SIBGRAPI conference on graphics, patterns and images, pp 221–228
53. Pinto A, Goldenstein S, Ferreira A, Carvalho T, Pedrini H, Rocha A (2020) Leveraging shape, reflectance and albedo from shading for face presentation attack detection. IEEE Trans Inf Forensics Secur 15:3347–3358
54. Kim Y, Yoo JH, Choi K (2011) A motion and similarity-based fake detection method for biometric face recognition systems. IEEE Trans Consum Electron 57(2):756–762
55. Liu S, Yang B, Yuen PC, Zhao G (2016) A 3D mask face anti-spoofing database with real world variations. In: Proceedings of the ieee conference on computer vision and pattern recognition workshops, pp 100–106
56. Bhattacharjee S, Mohammadi A, Marcel S (2018) Spoofing deep face recognition with custom silicone masks. In: IEEE international conference on biometrics theory, applications and systems (BTAS)
57. Galbally J, Satta R (2016) Three-dimensional and two-and-a-half-dimensional face recognition spoofing using three-dimensional printed models. IET Biom 5(2):83–91
58. Intel (2021). https://www.intelrealsense.com
59. Kose N, Dugelay JL (2013) On the vulnerability of face recognition systems to spoofing mask attacks. In: (ICASSP)international conference on acoustics, speech and signal processing. IEEE, pp 2357–2361
60. Liu S, Lan X, Yuen P (2020) Temporal similarity analysis of remote photoplethysmography for fast 3d mask face presentation attack detection. In: IEEE/CVF winter conference on applications of computer vision, pp 2608–2616
61. Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, Courville A, Bengio Y (2014) Generative adversarial nets. Adv Neural Inf Process Syst 27
62. Dolhansky B, Bitton J, Pflaum B, Lu J, Howes R, Wang M, Canton Ferrer C (2020) The deepfake detection challenge dataset. arXiv:2006.07397
63. Tolosana R, Vera-Rodriguez R, Fierrez J, Morales A, Ortega-Garcia J (2020) Deepfakes and beyond: a survey of face manipulation and fake detection. Inf Fusion 64:131–148
64. Hernandez-Ortega J, Tolosana R, Fierrez J, Morales A (2021) DeepFakesON-Phys: DeepFakes detection based on heart rate estimation. In: AAAI conference on artificial intelligence workshops
65. Singh R, Vatsa M, Bhatt HS, Bharadwaj S, Noore A, Nooreyezdan SS (2010) Plastic surgery: a new dimension to face recognition. IEEE Trans Inf Forensics Secur 5(3):441–448
66. Aggarwal G, Biswas S, Flynn PJ, Bowyer KW (2012)(2012) A sparse representation approach to face matching across plastic surgery. In: IEEE workshop on the applications of computer vision (WACV), pp 113–119
67. Bhattacharjee S, Mohammadi A, Marcel S (2018) Spoofing deep face recognition with custom silicone masks. In: International conference on biometrics theory, applications and systems (BTAS). IEEE
68. Raghavendra R, Raja KB, Busch C (2015) Presentation attack detection for face recognition using light field camera. IEEE Trans Image Process 24(3):1060–1075

69. Yi D, Lei Z, Zhang Z, Li SZ (2014) Face anti-spoofing: multi-spectral approach. In: Handbook of biometric anti-spoofing. Springer, pp 83–102
70. Lagorio A, Tistarelli M, Cadoni M, Fookes C, Sridharan S (2013) Liveness detection based on 3D face shape analysis. In: International workshop on biometrics and forensics (IWBF). IEEE
71. Sun L, Huang W, Wu M (2011) TIR/VIS correlation for liveness detection in face recognition. In: International conference on computer analysis of images and patterns. Springer, pp 114–121
72. Sluganovic I, Roeschlin M, Rasmussen KB, Martinovic I (2016) Using reflexive eye movements for fast challenge-response authentication. In: ACM SIGSAC conference on computer and communications security, pp 1056–1067
73. Chou CL (2021) Presentation attack detection based on score level fusion and challenge-response technique. J Supercomput 77(5):4681–4697
74. Kim Y, Na J, Yoon S, Yi J (2009) Masked fake face detection using radiance measurements. JOSA A 26(4):760–766
75. Yang J, Lei Z, Liao S, Li SZ (2013) Face liveness detection with component dependent descriptor. In: International conference on biometrics (ICB)
76. Galbally J, Marcel S, Fierrez J (2014) Image quality assessment for fake biometric detection: application to iris, fingerprint, and face recognition. IEEE Trans Image Process 23(2):710–724
77. Smith DF, Wiliem A, Lovell BC (2015) Face recognition on consumer devices: reflections on replay attacks. IEEE Trans Inf Forensics Secur 10(4):736–745
78. Li X, Komulainen J, Zhao G, Yuen PC, Pietikäinen M (2016) Generalized face anti-spoofing by detecting pulse from face videos. In: IEEE international conference on pattern recognition (ICPR), pp 4244–4249
79. Boulkenafet Z, Komulainen J, Li L, Feng X, Hadid A (2017) OULU-NPU: a mobile face presentation attack database with real-world variations. In: IEEE international conference on automatic face gesture recognition, pp 612–618
80. George A, Marcel S (2020) Learning one class representations for face presentation attack detection using multi-channel convolutional neural networks. IEEE Trans Inf Forensics Secur 16:361–375
81. Yu Z, Li X, Wang P, Zhao G (2021) TransRPPG: remote photoplethysmography transformer for 3d mask face presentation attack detection. IEEE Signal Process Lett
82. Zhang D, Ding D, Li J, Liu Q (2015) PCA based extracting feature using fast fourier transform for facial expression recognition. In: Transactions on engineering technologies, pp 413–424
83. Gonzalez-Sosa E, Vera-Rodriguez R, Fierrez J, Patel V (2017) Exploring body shape from mmW images for person recognition. IEEE Trans Inf Forensics Secur 12(9):2078–2089
84. Hernandez-Ortega J, Fierrez J, Morales A, Diaz D (2020) A comparative evaluation of heart rate estimation methods using face videos. In: IEEE conference on computers, software, and applications (COMPSAC)
85. Daza R, Morales A, Fierrez J, Tolosana R (2020) mEBAL: a multimodal database for eye blink detection and attention level estimation. In: ACM international conference on multimodal interaction (ICMI)
86. Pan G, Wu Z, Sun L (2008) Liveness detection for face recognition. In: Recent advances in face recognition. InTech
87. Wu HY, Rubinstein M, Shih E, Guttag J, Durand F, Freeman W (2012) Eulerian video magnification for revealing subtle changes in the world. ACM Trans Graph 31(4)
88. Liu A, Wan J, Escalera S, Jair Escalante H, Tan Z, Yuan Q, Wang K, Lin C, Guo G, Guyon I et al (2019) Multi-modal face anti-spoofing attack detection challenge at CVPR2019. In: IEEE/CVF conference on computer vision and pattern recognition workshops (CVPRw)
89. Zhang S, Wang X, Liu A, Zhao C, Wan J, Escalera S, Shi H, Wang Z, Li SZ (2019) A dataset and benchmark for large-scale multi-modal face anti-spoofing. In: IEEE/CVF conference on computer vision and pattern recognition (CVPR), pp 919–928
90. Ortega-Garcia J, Fierrez J, Alonso-Fernandez F, Galbally J, Freire MR, Gonzalez-Rodriguez J, Garcia-Mateo C, Alba-Castro JL, Gonzalez-Agulla E, Otero-Muras E et al (2010) The

multiscenario multienvironment biosecure multimodal database (BMDB). IEEE Trans Pattern Anal Mach Intell 32(6):1097–1111
91. Liu Y, Jourabloo A, Liu X (2018) Learning deep models for face anti-spoofing: Binary or auxiliary supervision. In: IEEE/CVF conference on computer vision and pattern recognition (CVPR), pp 389–398
92. Heusch G, George A, Geissbühler D, Mostaani Z, Marcel S (2020) Deep models and shortwave infrared information to detect face presentation attacks. IEEE Trans Biom Behav Identity Sci 2(4):399–409
93. Neves JC, Tolosana R, Vera-Rodriguez R, Lopes V, Proenca H, Fierrez J (2020) GANprintR: improved fakes and evaluation of the state of the art in face manipulation detection. IEEE J Sel Top Signal Process 14(5):1038–1048
94. Tolosana R, Romero-Tapiador S, Fierrez J, Vera-Rodriguez R (2021) DeepFakes evolution: analysis of facial regions and fake detection performance. In: IAPR international conference on pattern recognition workshops (ICPRw)
95. Dolhansky B, Howes R, Pflaum B, Baram N, Ferrer CC (2019) The DeepFake detection challenge (DFDC) preview dataset. arXiv:1910.08854
96. Chingovska I, Anjos A, Marcel S (2013) Anti-spoofing in action: joint operation with a verification system. In: Proceedings of the ieee conference on computer vision and pattern recognition workshops, pp 98–104
97. Fierrez J (2006) Adapted fusion schemes for multimodal biometric authentication. PhD Thesis, Universidad Politecnica de Madrid
98. de Freitas Pereira T, Anjos A, De Martino JM, Marcel S (2013) Can face anti-spoofing countermeasures work in a real world scenario? In: International conference on biometrics (ICB)
99. Fierrez J, Morales A, Vera-Rodriguez R, Camacho D (2018) Multiple classifiers in biometrics. Part 1: fundamentals and review. Inf Fusion 44:57–64
100. Ross AA, Nandakumar K, Jain AK (2006) Handbook of multibiometrics. Springer Science & Business Media