Chapter 9
Introduction to Face Presentation Attack Detection

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

Abstract The main scope of this chapter is to serve as a brief introduction to face presentation attack detection. 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, an artifact (generally a photograph, a video, or a mask) to try to impersonate a genuine user. First, we make an introduction of the current status of face recognition, its level of deployment, and the challenges it faces. In addition, we present the vulnerabilities and the possible attacks that a biometric 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. Later, 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 the vulnerabilities of face biometrics and developing effective countermeasures against known spoofs.

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

J. Hernandez-Ortega (✉)
Biometrics and Data Pattern Analytics - BiDA Lab, Universidad Autonoma de Madrid, Madrid, Spain
e-mail: javier.hernandezo@uam.es

J. Fierrez
Universidad Autonoma de Madrid, Madrid, Spain
e-mail: julian.fierrez@uam.es

A. Morales
School of Engineering, Universidad Autonoma de Madrid, Madrid, Spain
e-mail: aythami.morales@uam.es

J. Galbally
European Commission - DG Joint Research Centre, Ispra, Italy
e-mail: javier.galbally@ec.europa.eu

S. Marcel et al. (eds.), *Handbook of Biometric Anti-Spoofing*,
Advances in Computer Vision and Pattern Recognition,
https://doi.org/10.1007/978-3-319-92627-8_9

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, surveillance, smartphone authentication, forensics, and online services like e-learning and e-commerce.

Among all the existing biometric traits, face recognition is currently one of the most extended. The face has been studied as a mean of recognition since the 60s, acquiring special relevance in the 90s following the evolution of computer vision [1]. Some interesting properties of the human faces for biometrics are acquisition at a distance, nonintrusively, and the good discriminant characteristics of the face to perform identity recognition.

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

- Face is the second most largely deployed biometric at world level in terms of market quota right after fingerprints [2]. Each day more and more manufacturers are including face recognition in their products, like Apple with its Face ID technology.
- Face is adopted in most identification documents such as the ICAO-compliant biometric passport [3] or national ID cards [4].

Given their high level of deployment, attacks having a face recognition system as their target is not restricted anymore to theoretical scenarios, becoming a real threat. There exist all kinds of applications and sensitive information that can be menaced by attackers. Giving to each face recognition application an appropriate level of security, as it is being done with other biometric traits, 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 the verification and identification tasks, i.e., distinguishing better between subjects using the available information of their faces. To achieve that goal, a face recognition system should be able to optimize the differences between the facial features of each user [5], and also the similarities among samples of the same user. 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 area in face recognition research.

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 [6]. Regarding these security vulnerabilities, Presentation Attack Detection (PAD) consists on detecting whether a biometric trait comes from a living person or it is a fake.

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. Sections 9.5 and 9.6 discuss about architectures and applications of face PAD. Finally, concluding remarks are drawn in Sect. 9.7.

9.2 Vulnerabilities in Face Biometrics

In the present chapter, we concentrate on Presentation Attacks, i.e., attacks against the sensor of a face recognition system [7] (see point V1 in Fig. 9.1). An overview of indirect attacks to face systems can be found elsewhere [8]. Indirect attacks (points V2–V7 in Fig. 9.1) can be prevented by securing certain points of the face recognition system, i.e., the communication channels, the equipment and the infrastructure involved. The techniques needed for improving those modules are more related to "classical" cybersecurity than to biometrics, so they will not be covered in this chapter.

On the other hand, 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) to fraudulently access the biometric system.

A high amount of biometric data are exposed, (e.g., photographs and videos at 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 [9]. This is one of the well-known

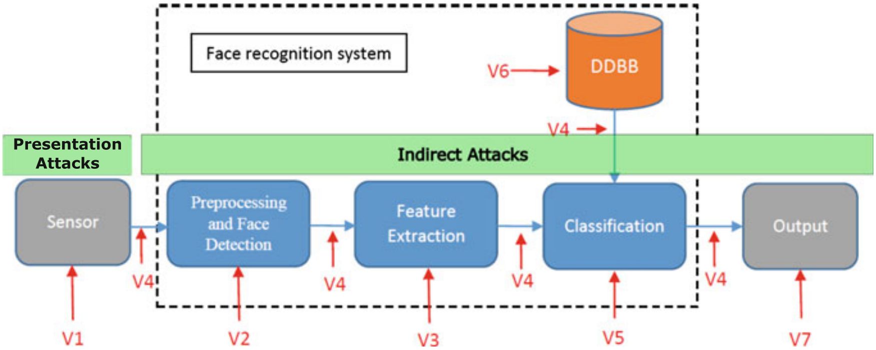

Fig. 9.1 Scheme of a generic biometric system. In this type of system, there exist several modules and points that can be the target of an attack (V1–V7). Presentation attacks are performed at sensor level (V1), without the need of having access to the interior of the system. Indirect attacks (V2–V7) can be performed at the database, the matcher, the communication channels, etc. In this type of attack the attacker needs access to the interior of the system

drawbacks of biometrics: “biometric traits are not secrets” [10]. In this context, it is worth noting that a factor that makes face an interesting trait for person recognition, i.e., easiness to capture, makes face biometrics also specially vulnerable to attackers, who may easily find example faces of the identities to attack.

In addition to being fairly easy to obtain a face image of the real users under attack, 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 [11].
2. Using a video of the user to be impersonated [12].
3. Building and using a 3D model of the attacked face, for example, an hyperrealistic mask [13].

The success probability of an attack may vary considerably depending on the characteristics of the face recognition system, for example, if it uses visible light or works in another range of the spectrum [14], if it has one or several sensors, the resolution, the lighting, and also depending on the characteristics of the artifact: 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 face recognition system 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 threats 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 [15, 16]; organization of competitions [17]; and acquisition of benchmark datasets [13, 18] that have resulted in the proposal of new presentation attack detection methods [7]; standards in the area [19, 20]; and patented PAD mechanisms for face recognition systems [21].

9.2.1 Attacking Methods

Typically, face recognition systems 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 face recognition system, such as

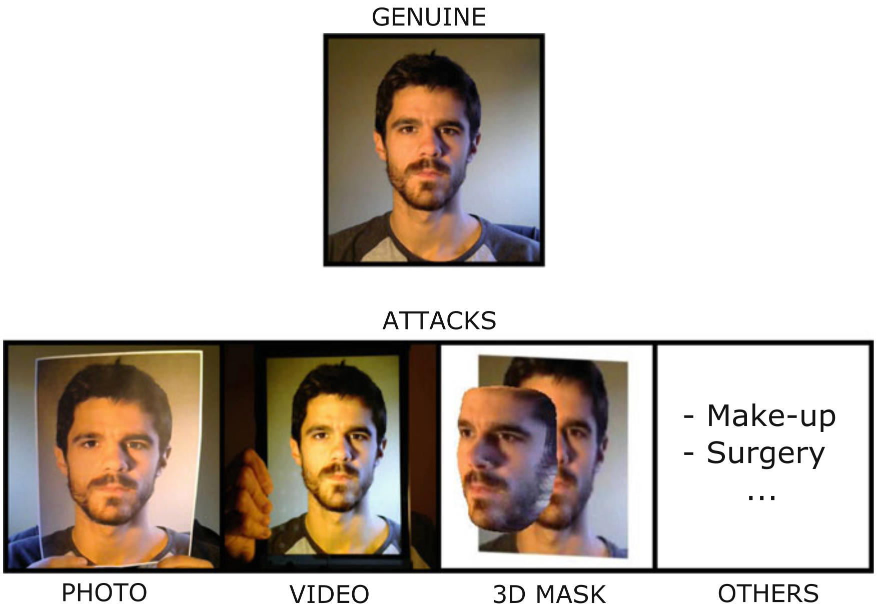

Fig. 9.2 Examples of face presentation attacks: The upper image shows an example of a genuine user, and below it there are some examples of presentation attacks, depending on the artifact shown to the sensor: a photo, a video, a 3D mask, and others

using makeup [22] or plastic surgery. However, using photographs and videos are 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 taking into account the nature and the level of complexity of the artifact 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 could exist more complex and newer attacks that may not fall into in any of these categories, or that may belong to several categories at the same time.

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 [23] (see example in Fig. 9.2).

Photo attacks are the most critical type of attack because of several factors. For example, 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 [24]. Alternatively, the photos can be displayed in the high-resolution screen of a device (e.g., a smartphone, a tablet, or a laptop). It is also easy to obtain samples of genuine faces thanks to the recent growth of social media sites like Facebook, Twitter, Flickr, etc. [9]. With the price reduction that digital cameras have experimented in recent years, it is also possible to obtain photos of a legitimate user simply by using a hidden camera.

Among the photo attack techniques, there are also more complex ones 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 [18]. This is a good way to avoid presentation attack detection techniques based on blinking and mouth movements detection.

Even if these attacks seem too simple to work in a real scenario, some studies performed by private security firms indicate that many commercial systems are vulnerable to them [25]. Due to the easiness of carrying out this type of attack, implementing robust countermeasures that perform well against them should be a must for any facial recognition system.

9.2.1.2 Video Attacks

Similarly 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 [26].

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 [27], (see Fig. 9.2). This type of attacks is often referred to in the literature as replay attacks, a more sophisticated version of photo attacks.

Replay attacks are more difficult to detect, compared to the photo spoofs, as not only the face texture and shape is emulated but also its dynamics, like eye blinking, mouth and/or facial movements [12]. 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 robust against photo attacks does not mean to be equally strong against video attacks [18]. Therefore, specific countermeasures need to be developed and implemented.

9.2.1.3 Mask Attacks

In this type of attack, the presented artifact 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 [28].

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:

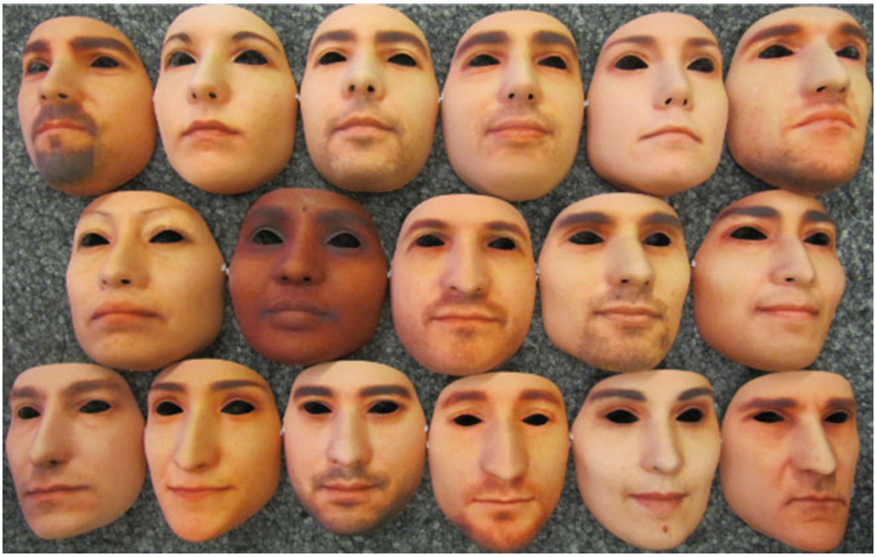

Fig. 9.3 **Example of 3D masks**. These are the 17 hard-resin facial masks used to create the 3DMAD dataset, from [13]

- 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. 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 two 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 (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 [29] (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 with the new generation of affordable 3D acquisition sensors [30].

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 reference [29] for a recent work evaluating face attacks with 3D-printed masks. There are some companies where such 3D face models may be obtained for a reasonable price.[1]

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 [13, 28, 29, 31].

9.3 Presentation Attack Detection

Face recognition systems try to differentiate between genuine users, not to determine if the biometric sample presented to the sensor is real or a fake. A presentation attack detection method is usually accepted to be any technique that is able to automatically distinguish between real biometric traits presented to the sensor and synthetically produced artifacts.

This can be done in four different ways [6]: (i) with available sensors to detect in the signal any pattern characteristic of live traits, (ii) with dedicated hardware to detect an evidence of liveness, which is not always possible to deploy, (iii) 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, or (iv) employing recognition algorithms intrinsically robust against attacks.

Due to its easiness of deployment, the most common countermeasures are based on employing the already existing hardware and running software PAD algorithms over it. A selection of relevant PAD works based on software techniques are shown in Table 9.1. A high number of the software-based PAD techniques are based on liveness detection without needing any special help of the user. This type of approach is really interesting as it allows to upgrade the countermeasures in existing systems without the requirement of new pieces of hardware, and permitting authentication to be done in real time as it does not need user interaction. These presentation attack detection techniques aim to detect physiological signs of life (such as eye blinking, facial expression changes, mouth movements, etc.), or any other differences between presentation attack artifacts and real biometric traits (e.g., texture and deformation).

There are works in the literature that use special sensors such as 3D scanners to verify that the captured faces are not 2D (i.e., flat objects) [32], or thermal sensors to detect the temperature distribution associated with real living faces [33]. However, these approaches are not popular, even though they tend to achieve higher presentation

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

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

Method	Year	Type of images	Database used	Type of features
[34]	2009	Visible and IR photo	Private	Color (reflectance)
[24]	2011	RGB video	PRINT-ATTACK	Face background motion
[12]	2012	RGB video	REPLAY-ATTACK	Texture based
[35]	2013	RGB photo and video	NUAA PI, PRINT-ATTACK and CASIA FAS	Texture based
[36]	2013	RGB photo and video	PRINT-ATTACK and REPLAY ATTACK	Texture based
[23]	2013	RGB video	PHOTO ATTACK	Motion correlation analysis
[37]	2014	RGB video	REPLAY-ATTACK	Image quality based
[38]	2015	RGB video	Private	Color (challenge reflections)
[39]	2016	RGB video	3DMAD and private	rPPG (color based)
[40]	2017	RGB video	OULU-NPU	Texture based
[41]	2018	RGB and NIR video	3DMAD and private	rPPG (color based)

detection rates, because in most systems the required hardware is expensive and not broadly available.

9.3.1 PAD Methods

The 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.

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) [12] or Gray-Level Co-occurrence Matrices (GLCM) followed by a learning stage to perform discrimination between textures.

Another group of methods exploits the fact that 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 [37].

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 [42], or working with images from outside the visible spectrum [43] 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 [34].

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.

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 of detecting any physiological sign of life, for example, pulse, eye blinking, facial expression changes, 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 presented artifacts 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 respect to the camera [23, 27]. 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 the user's head generally moves independently from the background.

Some works on dynamic analysis for face liveness detection are [44] or [35], which exploit the fact that humans blink on average three times per minute and analyzed videos to develop an eye blink-based presentation attack detection scheme.

Other works like [36] provide more evidence of liveness using Eulerian video magnification [45] 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 region that corresponds to the human heartbeat rate.

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 [38]. 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 complete databases to make recognition systems more robust to presentation attacks.

International competitions have played a key role to promote the development of PAD measures. These competitions include the IJCB 2017 Competition on Generalized Face Presentation Attack Detection in Mobile Authentication Scenarios [46], and the 2011 and 2013 2D Face Anti-Spoofing contests [17, 47].

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 [48] in order to correctly capture similar fake data than the present in real attacks (e.g., generation of multiple types of artifacts).
- Legal aspects: as in the face recognition field in general, data protection legislation limits the 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:

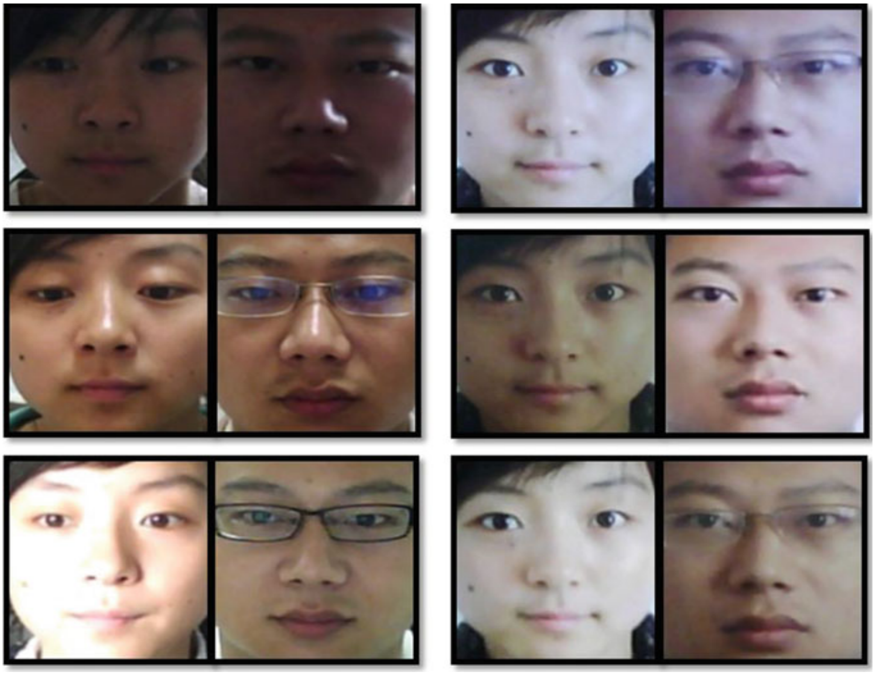

Fig. 9.4 Samples from the NUAA Photo Imposter Database [11]. Samples from two different users are shown. Each row corresponds to a different session. In each row, the left pair are from a live human and the right pair from a photo fake. Images have been taken from [11]

- The NUAA Photo Imposter Database (NUAA PI DB) [11] 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. 9.4. 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/xtan/data/nuaaimposterdb.html.
- The YALE-RECAPTURED DB [49] appeared shortly after, adding to the attacks of the NUAA PI DB also the difficulty of varying illumination conditions as well as considering LCD spoofs, not only printed photo attacks. The dataset consists of 640 static images of real access attempts and 1920 attack samples, acquired from 10 different users. The YALE-RECAPTURED DB is a compilation of images from the NUAA PI DB and the Yale Face Database B made by the University of Campinas.
- The PRINT-ATTACK DB [24] 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

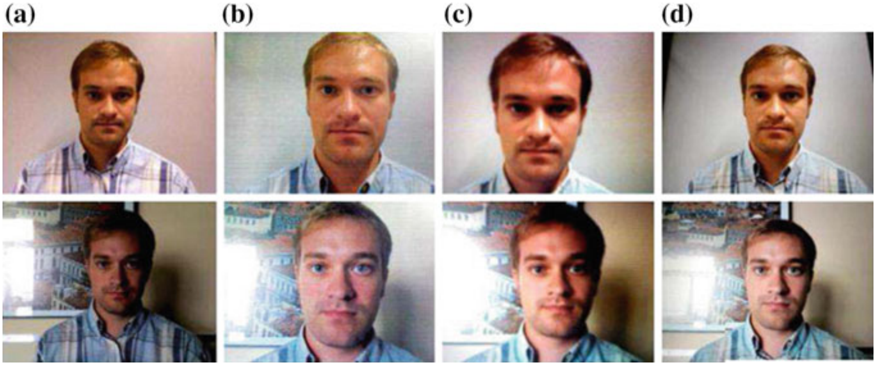

Fig. 9.5 Examples of real and fake samples from the REPLAY-ATTACK DB [12]. The images come from videos acquired in two illumination and background scenarios (controlled and adverse). The first row belongs to the controlled scenario while the second row represents the adverse condition. **a** Shows real samples, **b** shows samples of a printed photo attack, **c** corresponds to a LCD photo attack, and **d** to a high-definition photo attack

considers the case of photo attacks. It consists of 200 videos of real accesses and 200 videos of print attack attempts from 50 different users. Videos were recorded under two different background 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/dataset/printattack.

– The PHOTO ATTACK database [23] is an extension of the PRINT-ATTACK database. It also provides photo attacks with the difference that the attack photographs are presented to the camera using different devices such as mobile phones and tablets. It can be obtained at https://www.idiap.ch/dataset/photoattack.
– The REPLAY-ATTACK database [12], is also 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 video attacks using mobile phones and tablets. 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. 9.5. It can be obtained at https://www.idiap.ch/dataset/replayattack.

- The CASIA FAS DB [18], similarly to the REPLAY-ATTACK database contains photo attacks with different supports (paper, phones, and tablets) and also replay video attacks. The main difference with the REPLAY-ATTACK database is that while in the REPLAY DB only one acquisition sensor was used with different attacking devices and illumination conditions, the CASIA FAS DB was captured using sensors of different quality under uniform acquisition conditions. The CASIA FAS DB is property of the Institute of Automation, Chinese Academy of Sciences (CASIA), and it can be obtained at http://www.cbsr.ia.ac.cn/english/Databases.asp.

- The 3D MASK-ATTACK DB [13], as its name indicates, contains information related to mask attacks. As described above, all previous databases contain attacks performed with 2D artifacts (i.e., photo or video) that are very rarely effective against systems capturing 3D face data. The attacks in this case were performed with real-size 3D masks manufactured by ThatsMyFace.com[2] for 17 different subjects. 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 [29]. Example masks from this database can be seen in Fig. 9.3. The 3D MASK-ATTACK DB is property of the Idiap Research Institute, and it can be obtained at https://www.idiap.ch/dataset/3dmad.
- The OULU-NPU DB [40], is a recent dataset that contains information of PAD attacks acquired with mobile devices. Nowadays mobile authentication is one of the most relevant scenarios due to the widespread 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 5940 videos of 55 subjects recorded in 3 distinct illumination conditions, with 6 different smartphone models. The resolution of all videos is 1920 × 1080 including print and video replay attacks. The OULU-NPU DB is property of the University of Oulu, it has been used in the IJCB 2017 Competition on Generalized Face Presentation Attack Detection [46], and it can be obtained at https://sites.google.com/site/oulunpudatabase/.

In Table 9.2 we show a comparison of the most relevant features of the above-mentioned databases.

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 face recognition system can be done at different levels, namely score level or decision-level fusion [50].

The first possibility consists of using score level fusion as shown in Fig. 9.6. This is a popular approach due to its simplicity and the good results given in fusion of multimodal biometric systems [51–53]. 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 their 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

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

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 [11]	15/15	5,105/7,509	Photo	Held	Uncont.
YALE-RECAPTURED [49]	10/10	640/1,920	Photo	Held	Uncont.
PRINT-ATTACK[a] [12, 23, 24]	50/50	200/1,000	Photo and video	Held and fixed	Cont. and Uncont.
CASIA FAS [18]	50/50	150/450	Photo and video	Held	Uncont.
3D MASK-ATTACK [13]	17/17	170/85	Mask	Held	Cont.
OULU-NPU [40]	55/55	1,980/3,960	Photo and video	Mobile	Uncont.

[a] Containing also PHOTO-ATTACK DB and REPLAY-ATTACK DB

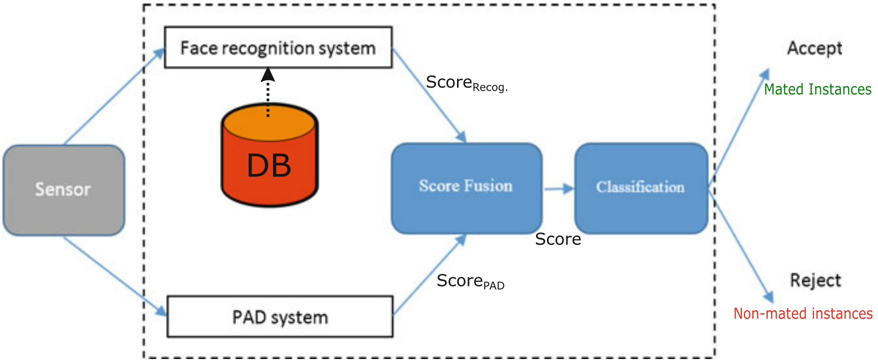

Fig. 9.6 Scheme of a parallel score level fusion between a PAD and a face recognition system. In this type of scheme, the input biometric data is sent at the same time to both the face recognition system and the PAD system, and each one generates an independent score, then the two scores are fused to take one unique decision

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. 9.7, 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 face recognition system will search for the identity that corresponds to the biometric sample knowing previously that the sample does not come from a presentation attack. On the other hand, in the serial scheme the average time for an access attempt will be longer due

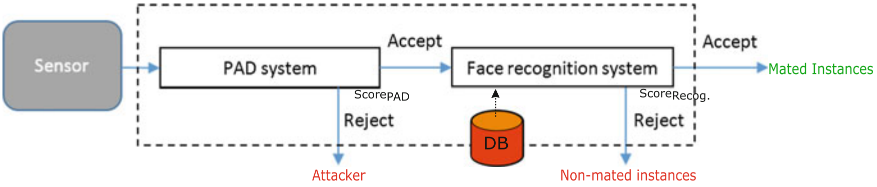

Fig. 9.7 Scheme of a serial fusion between a PAD and a face recognition system. In this type of scheme, the PAD system makes its decision first, and only if the samples are determined to come from a living person, then they are processed by the face recognition system

to the consecutive delays of the PAD and the face recognition modules. However, this approach avoids the extra work of the face recognition system in the case of a PAD attack, since the computation will end at an early stage.

9.6 Discussion

Attackers can use a great number of spoofs with no constraints, each one of different nature. Therefore, it is important 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 real attacking conditions in a laboratory evaluation. Under controlled conditions, systems are tested against a restricted number of typical presentation artifacts. These restrictions make it unfeasible to collect a database with all the different fake spoofs that may be found in the real world.

Normally, 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 fake artifacts (e.g., video replay attacks), 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 robust against particular types of artifacts, in order to develop fusion schemes that combine their results, achieving that way a high performance against a variety of presentation attacks [6, 51].

On the other hand, as technology progresses constantly, new hardware devices and software techniques continue to appear. It is important to keep track of this quick technological progress since some of the advances can be the key to develop novel and efficient presentation attack techniques. For example, focusing the research on the biological nature of biometric traits (e.g., thermogram, blood flow, etc.) should be considered [39], as the standard techniques based on texture and movement seem to be inefficient against some spoof artifacts.

9.7 Conclusions

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 is presentation attacks [6].

In this chapter, a review of the strengths and vulnerabilities of face as a biometric trait has been presented. 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 [7]. The weak points of the existing countermeasures have been discussed, and also some possible future directions to deal with those weaknesses have been commented.

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. Existing databases are useful resources to study presentation attacks, but the PAD techniques developed using them might not be robust in all possible attack scenarios. The combination of countermeasures with fusion schemes [52], and the acquisition of new challenging databases could be a key asset to counterfeit the new types of attacks that could appear [29].

To conclude this introductory chapter, it could be said that even though a great amount of work has been done to fight against face presentation attacks, there are still big challenges to be faced 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 done in the context of the TABULA RASA and BEAT projects funded under the 7th Framework Programme of EU, the project CogniMetrics (TEC2015-70627-R), the COST Action CA16101 (Multi-Foresee), and project Bio-Guard (Ayudas Fundación BBVA a Equipos de Investigación Científica 2017). Author J. H.-O. is supported by a FPI Fellowship from Universidad Autonoma de Madrid.

References

1. Turk MA, Pentland AP (1991) Face recognition using eigenfaces. In: Computer society conference on computer vision and pattern recognition (CVPR), pp 586–591
2. Biometrics: Market Shares, Strategies, and Forecasts, Worldwide, 2015–2021 (2015). Wintergreen Research, Inc
3. Gipp B, Beel J, Rössling I (2007) ePassport: The Worlds New Electronic Passport. Risks and its Security. CreateSpace, A Report about the ePassports Benefits
4. 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
5. Jain AK, Li SZ (2011) Handbook of face recognition. Springer, Berlin
6. 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
7. Galbally J, Marcel S, Fierrez J (2014) Biometric antispoofing methods: a survey in face recognition. IEEE Access 2:1530–1552

8. 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, Berlin, pp 358–365
9. Newman LH (2016). https://www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/
10. Goodin D (2008) Get your german interior ministers fingerprint here. Register 30
11. Tan X, Li Y, Liu J, Jiang L (2010) Face liveness detection from a single image with sparse low rank bilinear discriminative model. Comput Vis–ECCV 504–517
12. Chingovska I, Anjos A, Marcel S (2012) On the effectiveness of local binary patterns in face anti-spoofing. In: IEEE BIOSIG
13. Erdogmus N, Marcel S (2014) Spoofing face recognition with 3D masks. IEEE Trans Inf Forensics Secur 9(7):1084–1097
14. Gonzalez-Sosa E, Vera-Rodriguez R, Fierrez J, Patel V (2018) Person recognition beyond the visible spectrum: combining body shape and texture from mmW images. In: International conference on biometrics (ICB)
15. Proceedings of the IEEE international conference acoust. speech signal process. (ICASSP) (2017)
16. Proceedings of the IEEE/IAPR international joint conference biometrics (IJCB) (2017)
17. 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)
18. 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
19. 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
20. ISO: Information technology – biometric presentation attack detection – Part 1: Framework. international organization for standardization (2016). https://www.iso.org/standard/53227.html
21. Kim J, Choi H, Lee W (2011) Spoof detection method for touchless fingerprint acquisition apparatus. Korea Patent 1(054):314
22. Dantcheva A, Chen C, Ross A (2012) 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, pp 391–398
23. Anjos A, Chakka MM, Marcel S (2013) Motion-based counter-measures to photo attacks in face recognition. IET Biom 3(3):147–158
24. 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), pp 1–7
25. Nguyen D, Bui Q (2009) Your face is NOT your password. BlackHat DC
26. 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
27. 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
28. 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
29. 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
30. Intel: (2017). https://software.intel.com/realsense
31. 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

32. 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
33. 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, Berlin, pp 114–121
34. Kim Y, Na J, Yoon S, Yi J (2009) Masked fake face detection using radiance measurements. JOSA A 26(4):760–766
35. Yang J, Lei Z, Liao S, Li SZ (2013) Face liveness detection with component dependent descriptor. In: International conference on biometrics (ICB), pp 1–6
36. 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
37. 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
38. 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
39. Li X, Komulainen J, Zhao G, Yuen PC, Pietikäinen M (2016) Generalized face anti-spoofing by detecting pulse from face videos. In: 23rd international conference on pattern recognition (ICPR), IEEE, pp 4244–4249
40. 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
41. 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
42. 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
43. 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
44. Pan G, Wu Z, Sun L (2008) Liveness detection for face recognition. In: Recent advances in face recognition. InTech
45. 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)
46. 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
47. 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, Castrilln-Santana M, Määttä J, Hadid A, Pietikäinen M (2011) Competition on counter measures to 2-D facial spoofing attacks. In: International joint conference on biometrics (IJCB)
48. 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 (2010) The multiscenario multienvironment biosecure multimodal database (BMDB). IEEE Trans Pattern Anal Mach Intell 32(6):1097–1111
49. Peixoto B, Michelassi C, Rocha A (2011) Face liveness detection under bad illumination conditions. In: International conference on image processing (ICIP), pp 3557–3560
50. 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
51. 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), pp 1–8

52. Fierrez J, Morales A, Vera-Rodriguez R, Camacho D (2018) Multiple classifiers in biometrics. Part 1: Fundamentals and review. Inf Fusion 44:57–64
53. Ross AA, Nandakumar K, Jain AK (2006) Handbook of multibiometrics, Springer