Chapter 8
Face Recognition Systems Under Spoofing Attacks

Ivana Chingovska, Nesli Erdogmus, André Anjos and Sébastien Marcel

Abstract In this chapter, we give an overview of spoofing attacks and spoofing countermeasures for face recognition systems, with a focus on visual spectrum systems (VIS) in 2D and 3D, as well as near-infrared (NIR) and multispectral systems. We cover the existing types of spoofing attacks and report on their success to bypass several state-of-the-art face recognition systems. The results on two different face spoofing databases in VIS and one newly developed face spoofing database in NIR show that spoofing attacks present a significant security risk for face recognition systems in any part of the spectrum. The risk is partially reduced when using multispectral systems. We also give a systematic overview of the existing anti-spoofing techniques, with an analysis of their advantages and limitations and prospective for future work.

8.1 Introduction

Thanks to the growing availability of inexpensive cameras, as well as the unobtrusiveness of capturing procedures, face has a guaranteed position as one of the most exploitable biometric modes. Its wide deployment is further reinforced by the

I. Chingovska · A. Anjos · S. Marcel (✉)
Idiap Research Institute, Martigny, Switzerland
e-mail: sebastien.marcel@idiap.ch

I. Chingovska
e-mail: ivana.chingovska@idiap.ch

A. Anjos
e-mail: andre.anjos@idiap.ch

N. Erdogmus
Department of Computer Engineering, IZTECH, İzmir, Turkey
e-mail: neslierdogmus@iyte.edu.tr

T. Bourlai (ed.), *Face Recognition Across the Imaging Spectrum*,
DOI 10.1007/978-3-319-28501-6_8

rapid advancement of face recognition systems, which nowadays provide reliable recognition even under challenging conditions. Historically, 2D face recognition in the visual spectrum (VIS) has got the most attention and has reached a stage where it provides a secure, robust, and trustworthy biometric authentication at different security checkpoints: ID control systems, protected Web services, and even mobile devices. On the other hand, face recognition in 3D, near-infrared (NIR), and thermal spectrum shows an increased popularity in the recent years [1, 2].

Unfortunately, face recognition systems can be an attractive target for spoofing attacks: attempts to illegally access the system by providing a copy of a legal user's face. Information globalization acts in favor of such system misuse: users' personal data, including face images and videos, are nowadays widely available and can be easily downloaded from the Internet. Printed photographs of a user face, digital photographs displayed on a device, video replays, and 3D masks have already proven to be a serious threat for face recognition systems in VIS. Spoofing attacks for NIR face recognition systems have not received as much attention, but recent spoofing attempts indicate on their vulnerability too [3]. Considering that the driving force of attackers is not how hard systems are to spoof, but how valuable are the resources they guard, it is not pessimistic to expect more and more sophisticated spoofing attacks in near future.

In this chapter, we will cover research attempts in spoofing and anti-spoofing for the face mode from two perspectives. Firstly, we will investigate to what extent the state-of-the-art face recognition systems are vulnerable to spoofing attacks. This is a vital step toward verifying the threat and justifying the need of anti-spoofing methods. In addition, this step may reveal whether a spoofing attack database is relevant to be used to develop and evaluate anti-spoofing methods. We perform this analysis on four state-of-the-art face recognition systems working in VIS and NIR. In VIS, we exploit two different publicly available face spoofing databases, one with 2D attacks, and one with 3D mask attacks. To perform the analysis in NIR, we develop and present the first publicly available face spoofing database containing VIS and NIR spoofing attacks. By fusing the scores of the systems working in VIS and NIR, we extend the analysis to multispectral systems as well.

Secondly, we give an overview of the recent advancements in countermeasures to spoofing attacks for face recognition systems. This includes systematic categorization of the anti-spoofing methods and investigation on the attacks they are effective against. While there is a plethora of anti-spoofing methods for VIS face recognition systems, the amount of methods for NIR and multispectral systems is significantly smaller.

Unfortunately, it is extremely difficult to comparatively evaluate the performance of the existing anti-spoofing methods, mainly due to two factors. Firstly, very few of the research papers release the source code and the exact parameters to reproduce the presented results. Secondly, many of them are evaluated on private databases or are targeting just one type of spoofing attacks. Therefore, while we most often omit performance numbers, we distinguish methods whose results are fully reproducible on publicly available databases.

This chapter is organized as follows. We cover 2D face recognition systems in VIS and NIR under 2D spoofing attacks in Sects. 8.2.1 and 8.2.2, respectively. In Sect. 3, we cover face recognition systems in VIS under 3D spoofing attacks. Conclusions and discussion follow in Sect. 4.

8.2 Face Recognition Systems Under 2D Spoofing Attacks

8.2.1 Visual Spectrum (VIS) Face Recognition Systems

Numerous spoofing attack trials to test the robustness of commercial devices [4, 5], as well as several face spoofing databases have proved that face recognition systems in VIS can be spoofed with many different types of attacks. The attacks differ by their complexity, their cost and the amount of effort and skills required for producing them. The effectiveness of the attacks is closely related with these properties.

The spoofing countermeasures developed to protect 2D face recognition systems in VIS are by now developed to a very good extent, for example, the 2nd competition of countermeasures to 2D face spoofing attacks [6], where two of the submitted algorithms achieved perfect spoofing detection rate. The objective of this section is to summarize the research efforts in this direction, in terms of available spoofing attack types and databases, as well as existing solutions. We focus on face verification systems, where the spoofing attacks make most sense.

8.2.1.1 Types of Attacks and Databases

Probably, the simplest type of face spoofing attack is the print attack, which consists of printing a photograph of a valid user's face on paper. A more sophisticated type of attack involves presenting a digital photograph on the screen of a mobile device. These two types of attacks retain the face appearance, but present only a static face shows no signs of vitality. More sophisticated versions of the printed attacks simulate vitality by perforating the eye region or moving, rotating, and warping the printed paper [7–9]. In addition, there are video replay spoofing attacks, where a face video of a valid user is presented on the screen of a mobile device. Examples of spoofing attacks based on drawing of a user's face or using makeup to masquerade as a valid user have been registered at the ICB 2013 spoofing challenge.[1] Attacks with 3D masks will be covered in Sect. 3.

Besides the way of reproducing the spoofed face, the spoofing attacks can differ in a number of other criteria. For example, they can be recorded in controlled or uncontrolled environments. Furthermore, a fixed or a hand support can be used for

[1] http://www.biometrics-center.ch/testing/ tabula-rasa-spoofing-challenge-2013.

holding the spoof medium [10, 11] defines the term scenic 2D spoofing attack referring to attacks where the background content of the presented spoofing attack image is visible alongside the spoofed face. Finally, for some attacks, the border of the spoofing medium may be fully visible. The available face spoofing databases cover different subsets of these types of attacks. Different types of spoofing attacks pose a different level of difficulty to detect and are usually addressed with different types of countermeasures.

The number of face spoofing databases which are publicly available is limited. Up to the present moment, the established countermeasures to 2D face spoofing attacks have been evaluated either on private databases, or on three publicly available face spoofing databases: NUAA Photograph Imposter Database [8], CASIA Face Anti-spoofing Database (CASIA-FASD) [9] and the Replay-Attack family of databases [10]. NUAA database consists of attacks with printed photographs. It contains still images of real accesses and attacks to 15 identities and is recorded in three sessions under three different illumination conditions. When capturing the attacks, the photographs of the users are translated, rotated or warped.

CASIA-FASD provides videos of real accesses and three types of attacks to 50 identities. The first type is performed with printed photographs warped in front of the camera. The second type is printed photographs with perforated eye regions, so that a person can blink behind the photograph. The third type is a video playback of the user. When recording the database, three imaging qualities are considered: low, normal, and high.

The Replay-Attack family of databases consists of Print-Attack [12] containing printed photographs, Photo-Attack [13] containing printed and digital photographs, and Replay-Attack [10], as a superset of the previous two databases to which video attacks have been added. There is a total of 50 identities, recorded in both controlled and uncontrolled conditions, with diverse acquisition equipment.

Not all of the spoofing databases have equally wide applicability for evaluating anti-spoofing systems. For example, a database which offers still images, like NUAA, cannot be used for evaluation of countermeasures which require video inputs, like the motion-based algorithm described in Sect. 2.1.3. In addition, some databases are lacking a protocol to precisely define training, development, and test set. Finally, as described in Sect. 2.1.2, spoofing databases should provide enrollment samples which can be used to train and evaluate a baseline face verification system [14]. Both NUAA and CASIA-FASD suffer from this last drawback, and hence, their effectiveness in bypassing face verification systems cannot be properly evaluated. This disadvantage is overcome by the databases of the Replay-Attack family.

8.2.1.2 Assessing the Vulnerability

When evaluating a face verification system, it is a common practice to report False Acceptance Rate (FAR) (or False Match Rate (FMR)) and False Rejection Rate

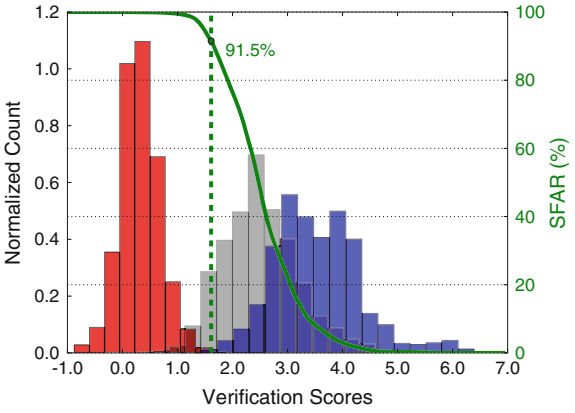

Fig. 8.1 Score distribution of GMM-based face recognition system for the samples in Replay-Attack. Real accesses: , zero-effort impostors: , and spoofing attacks:

(FRR) (or False Non-Match Rate (FNMR)).[2] The error rate at the point where these two values are equal is called Equal Error Rate (EER), while their average is called Half Total Error Rate (HTER). If the systems are exposed to spoofing attacks, their vulnerability is usually measured using Spoof False Acceptance Rate (SFAR) [14]. If the face verification system is tuned to work at particular operating point (decision threshold), SFAR gives the ratio of spoofing attacks whose score is higher than that point and are thus accepted by the system.

In order to be used for evaluation of verification systems, spoofing attack databases need to have properties that allow for their training [14]. In particular, they need to contain enrollment samples used to enroll clients in the verification systems. Out of the publicly available 2D face spoofing databases, only the Replay-Attack family satisfies this property. Using Replay-Attack database, we trained face verification system based on Gaussian mixture model (GMM), which extracts discrete cosine transform (DCT) features from the input images [17]. Figure 8.1 shows the distribution of the scores for the real accesses, zero-effort impostors and spoofing attacks from Replay-Attack for this system. The green line depicts the point which is chosen as a decision threshold based on EER criteria depending on FAR and FRR. The system shows a remarkable separability between the score distributions of the real accesses and zero-effort impostors, resulting in an almost perfect verification results (HTER = 0.14 %). However, the distributions of the scores of the real accesses and spoofing attacks overlap by a large extent. As a result, the system accepts 91.5 % of the spoofing attacks, which proves its high vulnerability to spoofing.

We performed similar analysis for three additional state-of-the-art face verification systems, each of which is based on different features and modeling paradigm. The first one uses local Gabor binary pattern histogram sequences (LGBPHS) [18],

[2]In their formal definition, FAR and FMR and FRR and FNRM are not synonymous [15]. However, they can be treated as such is some special cases, and we will do so, following the practice adopted in [16].

Table 8.1 Verification error rates and spoofing vulnerability of baseline face verification systems (in %)

System	FAR	FRR	SFAR
GMM	0.05	0.24	91.5
LGBPHS	1.47	2.13	88.5
GJet	0.28	0.24	95.0
ISV	0.00	0.17	92.6

the second one is based on Gabor jets comparison (GJet) [19], while the third one uses inter-session variability modeling (ISV) [20]. The results are shown in Table 8.1. All of the examined systems perform very well in the verification task. However, with SFAR of 90 %, each one of them exhibits a high vulnerability to spoofing, demonstrating the need for development of suitable countermeasures.

8.2.1.3 Spoofing CounterMeasures

The anti-spoofing methods for the face mode can be primarily categorized based on the type of data that is used to detect the spoofing attacks. In this respect, they can fall into two categories: hardware-based and software-based [21]. The hardware-based solutions use additional hardware to detect the spoofing attacks, which may be a thermal or near-infrared camera, 3D sensor, etc. The software-based ones utilize solely the information which is captured by the camera of the recognition system and try to directly exploit the characteristic of the input images.

Some of the software-based methods require, either implicitly or explicitly, that the user answers to some kind of interactive challenge. Yet, most of these methods take the decision in a non-intrusive manner, without any requirement for an explicit input from the user. They use different types of cues that may indicate the presence of a live subject in front of the system: liveness, motion, visual appearance, contextual information, and 3D reconstruction information. Usually, the features extracted for these purposes are handcrafted based on prior knowledge about the task; however, there are algorithms which extract relevant features in a completely data-driven fashion.

In the remainder of this section, we are going to cover the most prominent representatives of face anti-spoofing methods and make a comparative analysis of their performance and limitations. We will put an additional note to those which depend on interaction with the user.

Before proceeding, it is important to notice that several researchers have made attempts to increase the robustness of biometric recognition systems to spoofing attacks by using multiple biometric modes [22]. The intuition behind these solutions is that an attacker may need more effort to spoof the system, because she needs to spoof more modes. Within such multimodal framework, face has been combined with fingerprint and iris [23–26], or with voice [27]. [23–26] have proven, however, that poorly designed combination rules for multimodal systems may

not be helpful. Combination rules designed specifically for the purpose of increased robustness have been designed in [25, 26].

Liveness Detection

The liveness detection anti-spoofing methods base their decision on the evidence of liveness present on the scene. Usually, eye-blinking, mouth movements, and in-voluntary subtle head movements are considered as evidence of liveness. One of the first attempts to employ eye-blinking for anti-spoofing is performed by [28], which uses conditional random fields (CRF) to model the state of the eye as open or closed and the correlation between its state and the observation. With a similar purpose, [29] uses active shape models to detect the eye contours and difference of images to detect the blinking activity. In [30], eye-blinking detection is combined with the analysis of the 3D properties of the subject.

A key, but limiting assumption of the liveness detection methods, is that the subject will experience the actions that suggest liveness within a given short time frame. For example, [28] assumes that eye blinks happen every 2–4 s, which may not be true always and for all the subjects. To be fully successful, these methods depend on user input like deliberate eyeblinks, which may give them a level of intrusiveness.

An attempt to overcome this limitation is done by methods which rely on more subtle changes in the face region, including color changes due to blood flow. To be able to detect these changes, [31] performs Eulerian motion magnification [32] as a preprocessing before applying a technique for analyzing the texture or the motion patterns.

Another drawback of the liveness methods is that, although they may be successful in the case of print and attacks (even when they are warped or rotated [28]), they may be easily deceived by spoofing attacks where liveness evidence is present, like video playback or 3D masks.

Motion Analysis

The motion-based methods try to find properties of the motion patterns of a person in front of the system, in order to distinguish them from motion patterns in the presence of a spoofing attack. A few of these methods base their approach on the assumption that a person's head, being a 3D object, moves differently than a 2D spoofing attack displayed on a planar media. For example, [33] uses optical flow method to track movements on different face parts. The authors assume that, in contrast to a face displayed on a 2D surface, a 3D face will generate higher amount of motion in central face parts closer to the camera (like the nose) then in the face parts which are further away from the camera (like the ears). Furthermore, a 3D face exhibits motion flows which are in opposite directions for central and peripheral face parts. On the other hand, [34] derives a heuristics for the optical flow field for four basic 2D surface motion types: translation, in-plane rotation, panning, and swing. On the contrary, a 3D face and facial expressions generate irregular optical flow field.

Another set of motion-based methods assumes a high correlation between the movements in the face region and the background in the case of a spoofing attack. Such a correlation is unlikely in the case of a real access. [12] bases the computation of the correlation on 10 quantities extracted from the face region and the background. For the same purpose, [13] relies on quantization of optical flow motion vectors, while [35] performs foreground–background consistency analysis.

Similarly to the liveness detection methods, the motion analysis approaches depend on the subtle involuntary movements of the user. In addition, sometimes they capture the motion introduced by an attacker who holds the attack media with his hands. If the presumed motion patterns are absent during the short acquisition process (e.g., a very still person who does not blink), the methods may fail. These methods are mostly targeting photograph spoofing attacks and will most likely fail in case of spoofing attacks by video playbacks or 3D masks. Furthermore, the methods based on motion correlation are particularly directed for scenic 2D spoofing attack, where the background of the spoofed image is visible.

Visual Appearance

The anti-spoofing methods analyzing the visual appearance stand behind a strong argumentation about the differences in the visual properties of real accesses and spoofing attacks, explained in a number of publications. Firstly, a real face and the human skin have their own optical qualities (absorption, reflection, scattering, refraction), which other materials that can be used as spoofing media (paper, photographic paper, or electronic display) do not possess [36]. Similar differences can appear as a result of the diffuse reflection due to a non-natural shape of the spoofing attacks [37]. Limited resolution of the device used for spoofing or the involuntary shaking of the spoofing media may cause a blurring in the case of spoofing attacks [37–39]. Artifacts appearing in the spoofing production process, like jitter and banding in the case of print attacks [35, 39] or flickering and Moire´ effect in the case of video attacks [40] are yet another sources of differences between the real accesses and spoofing attacks. Many of these visual properties are indistinguishable for the human eye, but often can be easily extracted using different image processing and computer vision algorithms.

The first approach leveraging on the argument that spoofing attacks are usually of lower resolution and thus contain less high-frequency components is proposed in [38]. The proposed feature vector is based on analysis of the 2D Fourier spectrum of the input image and its energy change over time. Instead of comparing the high-frequency content of the input, [8] and [9] base their discrimination on the high-middle band of the Fourier spectrum, which is extracted using difference of Gaussians (DoG) method.

Some publications assume that the differences between real accesses and attacks are most prominent within the reflectance component of the input image and estimate it in different ways: [8] uses the Lambertian reflectance model [41] and Variational retinex-based method, while [42] uses dichromatic reflection model. Then, [8] classifies the obtained features using sparse low rank bilinear discriminative model, while [42] compares the gradient histograms of the reflectance images.

A feature set inspired by a physics-based model for recaptured images, which reveals differences in the background contextual information, reflection, surface gradient, color, contrast, chromaticity, and blurriness, is created by [43]. Different sets of visual features related to texture, color, edges, and/or gradient are used by [44, 45]. [46] generalizes the appearance differences into quality differences and uses a feature vector composed of 25 different image quality measures.

Several publications make use of specific computer vision descriptors for texture analysis. Local binary pattern (LBP) [47] appears to be the most significantly exploited for the purpose of anti-spoofing, both in its single resolution [10] and multiresolution [37, 39, 48] variants. Histogram of oriented gradients (HOG) [37, 39, 44], gray-level co-occurrence matrix (GLCM) [44], Haar wavelets [35], and Gabor wavelets [39] are some of the other alternatives.

More recently, the analysis of the visual appearance has been enhanced into a temporal domain. In [40], the authors firstly extract the noise from each video frame and then summarize the relevant components of its 2D Fourier analysis into the so-called visual rhythm image. The properties of this image are then captured using GLCM. The method proposed in [49] utilizes LBP-TOP [50], where instead of LBP analysis on a single frame, dynamical LBP analysis on a frame and its neighboring frames is performed.

The methods described before present different rates of success, which cannot be easily compared because they are obtained on different types of attacks and usually on databases which are not released publicly. An interesting property of the majority of the visual appearance methods is that they can work even if only a single image is available at input. They are usually applied either on the face bounding box, face parts, or on the full input image. As one of their advantages, they are very user-friendly and non-intrusive and do not depend on the behavior of the user (unlike the liveness detection and motion analysis methods). Furthermore, an attack which can deceive them a priori has not been presented up to this moment. For example, they can be expected to successfully detect print, photograph, video, or even 3D mask attacks. Yet, their success may be put into question if the spoofing attacks are printed or displayed on high-resolution media, thus lacking some of the artifacts that these methods rely on. Their generalization properties when applied to different acquisition conditions or new types of attacks are also uncertain, since the visual appearance of the input images often depends on the light condition, acquisition devices, or display media.

Contextual Information

The context of the scene present as a background information in front of the recognition system is used as a cue to detect spoofing attacks. In [7], the authors notice that in the case of a spoofing attack, there will be a change in the contextual information of the background when the face appears. To detect such changes, the authors compare the regions around reference fiducial key points in the region around the face.

The approach presented in [51] is targeting attacks where the contextual information consists of the border of the spoofing medium. Hence, a prerequisite is that

the spoofing medium is fully visible to the system. The method relies on HOG [52] to detect upper body and spoofing medium borders.

3D Information

The 3D property of a human face is a cue that unambiguously distinguishes real accesses from 2D spoofing attacks. This is used by several publications, which try to reconstruct or estimate the 3D information from the user's face. For example, [53] recovers and classifies the 3D structure of the face based on two or more images taken from different viewing angles. For similar purposes, [54] uses 3D projective invariants of a moving head. The disadvantage of these approaches is their intrusiveness: The user needs to be collaborative and moves his head to a different angle in the first case, or performs certain movements at random intervals in the second case. Avoiding such a constraint, [55] estimates the focus variabilities between two images taken consecutively and focused on different parts of the face. In the case of a 2D spoofing attacks, it is expected that focus variabilities will be absent.

It is important to note that the success of this set of methods is usually limited to 2D spoofing attacks and is likely to fail 3D mask attacks.

Challenge–Response Unlike the majority of motion analysis of liveness detection methods which rely on the involuntary movements of the user, challenge–response anti-spoofing methods explicitly ask the user to perform certain action to verify his liveness. Representatives of this type have been already mentioned [53, 54]. There are various types of challenges that a user can perform: taking a particular head pose [56] or following a moving point with a gaze [57] are some of them. Finding the static and dynamic relationship between face and voice information from a speaking face or modeling a speaker in 3D shape is an option for anti-spoofing in a multimodal audio-visual system [58]. It is important to note that the last approach can successfully detect not only visual, but even audio-visual spoofing attacks, such as video playbacks with recorded utterance or 3D synthetic talking heads.

The challenge–response methods are considered to be intrusive, non-friendly, and uncomfortable from the aspect of a user experience. In addition, they usually require that the authentication is performed during a prolonged time span. Finally, they are not transparent for the user. In this way, it is possible for a malicious user to guess the liveness cue and try to bypass it.

Feature Learning

Following a recent trend, the anti-spoofing community started experimenting with approaches where the anti-spoofing features are automatically learned directly from the data. This is in contrast to the previously discussed approaches, where the features are inspired by some particular characteristics that can be observed as common either for real accesses or for some types of spoofing attacks. It is argued, however, that the features engineered in this way are not suitable for different kinds of spoofing attacks [59, 60]. Both [60] and [59] are training a convolutional neural network (CNN) for the purpose. In [60], experiments with face images in 5 different

resolutions are given, while in [59], the authors use an optimization procedure to select the best CNN to learn the features, out of a family of CNNs with different hyper-parameters.

Hardware-Based Methods

The hardware-based methods employ an additional piece of hardware along the camera used by the recognition system. These methods detect spoofing attacks using the cues captured by the additional hardware. For example, very often, these methods exploit the properties of the human body in different regions of the electromagnetic spectrum. In such a case, the additional hardware may refer to the sensor used to capture data at a particular wavelength, a light filter which is applied to the camera, or illuminator emitting light at a particular wavelength. Most often, the infrared (IR) region of the electromagnetic spectrum is used, from long wavelength (thermal IR) to NIR.

The idea originates from informal experiments presented in [61]. The paper presents examples of face images of individuals, taken in the long-wavelength infrared region of the spectrum (8−15 μm), also known as thermal infrared region. The images represent the thermal emissions naturally coming from the human body. Depending on the spoofing attack material, these thermal emissions can be significantly reduced if an individual holds the spoofing attack in front of the face.

Operating in the NIR spectrum [62] suggests that there is an apparent difference between the reflectance property of the human skin and other materials. [63] analyzes the reflectance properties of skin and artificial materials at two wavelengths: one in NIR and one in visual spectrum. The two obtained measurements form a feature vector for a multispectral-based spoofing detection. Trying to overcome the requirement for a particular distance from the sensor in [63, 64] finds the most suitable wavelengths and trains the system with data taken at multiple distances. In [65], the authors use multispectral filters to obtain an image which presents the different radiometric response of different parts of the face under a full-spectrum active light. The distinction between real accesses and spoofing attacks is made by analyzing the gradient of the image.

Going back to the visual spectrum, [66] measures the reflectance of the skin using a high-resolution, high-accuracy spectrograph. Using 8 different wavelengths in the visual spectrum, [67] creates a feature vector based on the RGB values of the obtained images.

It is important to notice that in the scenarios referred to in this section, the hardware-based methods using IR sensors are used to protect face recognition system in the visual spectrum. However, these methods are even more suitable to operate alongside face recognition systems in the IR spectrum. IR and multispectral face recognition systems will be covered in Sect. 2.2.

Another example of a hardware-based method is the recent approach [68] which uses, the newly developed light-field camera that records the direction and intensity of each light ray. This camera renders multiple focus images in a single shot. Using this technology, it is possible to distinguish between the multiple focus levels to distinguish between 2D spoofing attacks and real faces.

The need of an additional hardware renders the hardware-based method more expensive and less convenient from deployment perspective. This requirement implies that some of them cannot be used in certain applications, for example, mobile systems.

Fusion

The main motivation behind approaches proposing fusion of anti-spoofing methods is the fact that different types of spoofing attacks have different properties and it is difficult to address all of them only with a single feature type or method. In addition, [69] has made a proof of concept that the anti-spoofing systems are unable to generalize well on unseen spoofing attacks. The discussion in the previous sections, where we state which spoofing attacks are most likely to be detected by the various categories of methods, is an argument toward this direction. Hence, there is an emergence of a trend of fusing several different anti-spoofing methods to obtain a more general countermeasure effective against a multitude of attack types.

The first attempts of fusing have been performed by [45], where the authors develop a fusion scheme at a frame and video level and apply it to a set of visual appearance cues, and [44], where the fusion of visual appearance cues is done at feature level. The authors in [35] for the first time bring the intuition that the fusion can have a bigger impact if done with complementary countermeasures, i.e., those that address different types of cues at the spoofing attacks. In the particular case, although subject to some prerequisites of the videos, motion analysis method is fused with a visual appearance method.

To measure the level of independence of two anti-spoofing systems, and thus to get a measurement of the effectiveness of their fusion, [69] proposes employing a statistical analysis based on [70]. For the same purpose, [11] proposes to count the common error rates [11] further shows that fusing several simple anti-spoofing methods which do not involve complex inefficient classifiers may be favorable with respect to a single one which is memory and time requiring.

The trend of fusing multiple complementary anti-spoofing methods continued with [6]. While fusion at score level is the most dominant approach, future efforts should analyze what is the most effective fusion strategy, both in terms of error rates, and flexibility of incorporating a newly developed countermeasure into the fused system.

8.2.1.4 Discussion

2D spoofing attacks in VIS have attracted a lot of interest among researchers in the past years. This resulted in a large set of countermeasures belonging to different categories, with different efficiency and targeting different types of attacks. Besides this, the countermeasures differ in other important properties, such as their intrusiveness and the type of input they require. We believe that summarizing the available methods based on their properties is much more important than comparing their performance, because each one is tested and works on different conditions. For

this purpose, we systematized them in Table 8.4, grouping them by category and listing their main properties. In this way, a user can decide which method to use based on the expected spoofing attacks, types of input the system provides, as well as ease of implementation and convenience of use.

From the results published in the literature so far, we can deduce two main conclusions which may serve to direct future research.

1. Many publications have already achieved close to zero or zero error rates in spoofing detection for the three main publicly available face spoofing databases. The community has recognized the limitations of the currently existing databases, ranging from small number of identities, to small set of spoofing attack types, to various types of biases. More challenging databases need to be created in future. Considering different materials to produce the spoofing attacks, using better quality equipment, creating more diverse illumination conditions and recording more clients are some of the ways to add to the adversity of the spoofing databases.
2. Several publications have shown that the proposed anti-spoofing methods do not generalize well on new spoofing attacks not seen during training time [60, 69]. However, good generalization capabilities should be a key feature for the anti-spoofing methods, as new types of spoofing attacks can never be anticipated. Therefore, future research effort should put an emphasis on methods which generalize well over multitude of different types of spoofing attacks.

8.2.2 NIR and Multispectral Face Recognition Systems

The face recognition systems which work in the infrared part of the spectrum have one major advantage over their counterparts in the visible spectrum: They are usually invariant to illumination changes in the environment. The thermal imaging face recognition systems capture the thermal emissions naturally coming from the human body [2] and use their pattern to recognize individuals. They are naturally resistant to any kind of 2D spoofing attacks, as the thermal signatures of 2 individuals are different [61]. Even more, such systems are resistant to surgically performed face alterations, because tissue redistribution, addition of artificial materials, and alteration of blood vessel flows that may happen during a surgery have a big impact on the thermal signature of a person [62]. Therefore, spoofing attacks for thermal imaging face recognition systems are out of the scope of this chapter.

On the other hand, the NIR face recognition systems need an active NIR light to illuminate the subject and capture the reflection of the face under that light. Examples of the robustness of these systems have been demonstrated in [71, 72]. Multispectral systems are created by fusing face recognition systems which work in different part of the spectrum, such as NIR and thermal, or NIR and VIS [2]. However, the robustness to spoofing attacks of these systems has been addressed very sparsely.

The objective of this section is to study several examples of face recognition systems working in NIR and to evaluate their vulnerability to a basic type of spoofing attacks. We present a new publicly available multispectral face spoofing database, containing face images in NIR and VIS spectrum. The systems are evaluated when working in VIS and NIR spectrum, as well as in multispectral scenario, by fusing the scores of the VIS and NIR systems.

8.2.2.1 Types of Attacks and Databases

The attempts to spoof face recognition system in NIR spectrum are by far less numerous than similar attempts in visual spectrum. The work in [62] presents a way to use NIR technology to detect spoofing attacks for visual spectrum face recognition systems. Some of them even present an empirical study on the success in detecting spoofing attacks. However, none of these studies creates and evaluates spoofing attacks designated to NIR and/or multispectral face recognition systems. That is, in fact, a basic preliminary step before developing a countermeasure.

To the best of our knowledge, only [3] has studied the effect of spoofing attacks on NIR and multispectral face recognition system. The authors develop a database with 100 clients, taking simultaneously visual spectrum and NIR images at each shot. Then, spoofing attacks are created from part of the recorded images in the two spectra, by printing them on a coarse paper. In this way, both visual and NIR spoofing attacks are created. A disadvantage of the study on [3] is that the database is not publicly available.

To alleviate this issue, we created a new publicly available database, called Multispectral-Spoof.[3] The total number of clients in the database is 21. The database is recorded using a uEye camera with CMOS monochrome sensor and a resolution of 1280 × 1024. The images in NIR were recorded using a NIR illuminator and a NIR cut filter of 800 nm attached to the camera. The images were taken in 7 different conditions: one in an uncontrolled hallway environment and 6 in office environment with natural light, ambient light, no light, illuminator spotlight from the left and from the right, and 2 illuminator spotlights. 5 images in visual spectra and 5 images in NIR were taken under each of these conditions.

Bearing in mind that the attacker may have an access to the best-quality real access samples of the clients, we selected the 3 best images from the visual and NIR samples of each client and printed them in black and white on a normal A4 paper, using a printer with 600 dpi. Then, using the same settings as before, we recorded the printed spoofing attacks in both visual and NIR spectrum in 3 different lighting conditions in an office environment: natural light, ambient light, and 2 illuminator spotlights. For an unbiased evaluation, the clients in the database are divided into 3 non-overlapping sets for training (9 clients), development (6 clients), and testing

[3]The link to download the database, together with manual face annotations, will be available as soon as this book chapter is accepted for publication.

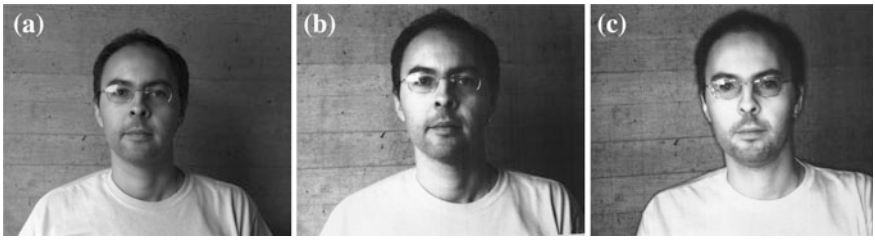

Fig. 8.2 Real and spoofing attack samples from the database recorded in VIS. **a** Real access. **b** VIS attack. **c** NIR-attack

Fig. 8.3 Real and spoofing attack samples from the database recorded in NIR. **a** Real access. **b** VIS attack. **c** NIR-attack

(6 clients) purposes. Figs. 8.2 and 8.3 illustrate examples of real access and attack samples taken in VIS and NIR, respectively.

8.2.2.2 Assessing the Vulnerability

In this section, we study the effectiveness of VIS and NIR spoofing attacks in defeating VIS and NIR recognition systems. We would like to inspect whether it is possible to spoof VIS systems using NIR attacks and vice versa. First insight into this problem has been reported by [3]. The studied face recognition system [71] is based on Gabor wavelets. The authors conclude that while VIS system is vulnerable to VIS attacks and NIR system is vulnerable to NIR attacks, there are little chances that VIS attacks can bypass a NIR system and vice versa.

We perform similar analysis using the publicly available Multispectral-Spoof database. We analyze the same recognition systems described in Sect. 2.1.2: GMM, LGBPHS, GJet, and ISV, this time operating in two domains: VIS and NIR.[4]

The Multispectral-Spoof database contains a total of 1680 real access images (840 in VIS and 840 in NIR), as well as 3024 spoofing attack images (756 VIS and 756 NIR attacks for each of the two systems). To allow for training and evaluation

[4]The link to fully reproduce the results obtained here will be available as soon as this book chapter is accepted for publication.

of face recognition systems and following the example of Replay-Attack, 10 of the images of each client are reserved for enrollment purposes. During the evaluation, the vulnerability of each of the systems (VIS and NIR) when exposed to the two types of attacks (VIS and NIR) was assessed.

Independent VIS and NIR Systems

We firstly analyze the verification performance and the vulnerabilities of GMM-based system working in VIS mode. The score distributions for this system are given in Fig. 8.4, and the good separation between the distribution of the real accesses and spoofing attacks indicates that the system behaves relatively well in verification. However, Fig. 8.4a shows that the system is highly vulnerable to spoofing attacks recorded in VIS. More surprisingly, Fig. 8.4b shows that the system can be spoofed even with spoofing attacks taken in NIR spectrum, with probability of 30.56 %.

Figure 8.5 demonstrates similar analysis when the GMM-based system works in NIR mode. Again, the system shows relatively good verification performance. In this case, the system shows low vulnerability to VIS attacks, amounting to 13.96 %. The vulnerability to NIR attacks, however, goes as high as 71.8 %.

Table 8.2 presents the verification results and the vulnerabilities for the rest of the studied face recognition systems. All of them are moderately to highly vulnerable to spoofing attacks recorded in the spectrum that they operate in. For example, SFAR for VIS systems to VIS attacks ranges from 59.26 to 74.07 %. In NIR mode, the systems are even more vulnerable to NIR attacks: SFAR ranges from 71.76 to 88.89 %. As can be expected, the vulnerability to attacks recorded in the other spectrum than the one the systems work in is much lower. However, it still amounts to a considerable SFAR, especially in the case of VIS system: the SFAR for NIR attacks is between 27.78 to 38.89 %. Among the studied systems, GJet appears to be the most vulnerable, while ISV shows the greatest robustness to spoofing attacks, both in VIS and NIR mode.

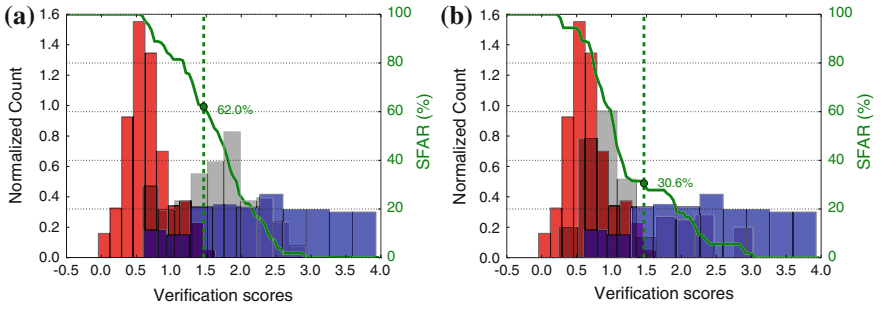

Fig. 8.4 Score distribution of GMM-based face recognition system for the samples in Multispectral-Spoof: VIS mode. Real accesses: ; zero-effort impostors: ; and spoofing attacks: . **a** VIS attack. **b** NIR-attack

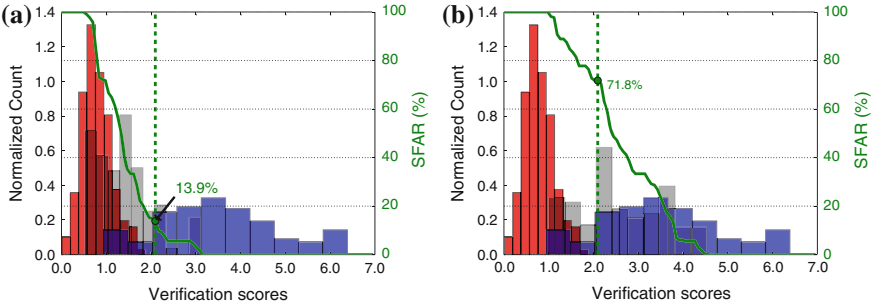

Fig. 8.5 Score distribution of GMM-based face recognition system for the samples in Multispectral-Spoof: NIR mode. Real accesses: ; zero-effort impostors: ; and spoofing attacks: . **a** VIS attack. **b** NIR-attack

Table 8.2 Verification error rates and spoofing vulnerability of baseline face verification systems (in %)

	VIS system				NIR system			
System	FAR	FRR	SFAR		FAR	FRR	SFAR	
			VIS attack	NIR attack			VIS attack	NIR attack
GMM	0.78	15	62.04	30.56	0	13.96	13.89	71.76
LGBPHS	13.11	3.33	69.44	54.17	4.13	11.17	25.93	74.07
GJet	9.89	6.11	74.07	38.89	3.35	6.15	27.78	88.89
ISV	1.44	16.67	59.26	27.78	0	12.29	14.81	72.22

Multispectral System

The analysis presented in [3] is extended to a multispectral system by fusing the scores of the attacks on the two systems. If simple SUM rule is used for the score fusion, the multispectral system appears to be vulnerable to any of the two types of spoofing attacks.

In our case, we investigate three different strategies to fuse the scores of VIS and NIR systems: SUM of scores, linear logistic regression (LLR), and polynomial logistic regression (PLR). The vulnerabilities of the GMM-based system working in multispectral mode are given in Table 8.3.

The results show that the vulnerability of the multispectral system is highly reduced, especially to VIS spoofing attacks. The vulnerability to NIR spoofing

Table 8.3 Verification error rates and spoofing vulnerability of multispectral GMM-based system (in %)

Fusion method	FAR	FRR	SFAR	
			VIS attack	NIR attack
SUM	0	11.17	11.11	33.02
LLR	0	14.53	9.26	25.12
PLR	0	10.06	9.72	53.95

attacks is reduced to a lesser extent. However, the obtained SFAR has moderately high level and suggests that VIS and NIR spoofing attacks present a considerable security threat even for multispectral systems. The results for the other face recognition systems (LGBPHS, GJet and ISV) bring to similar conclusions.

8.2.2.3 Discussion

Research on spoofing and anti-spoofing for NIR and multispectral face recognition system is still in its infancy. We contribute to the attempts to spoof such systems by creating a publicly available VIS and NIR face spoofing database that can be used in a multispectral setting as well. From our initial experiments, we see that it is possible to spoof VIS and NIR systems with both VIS and NIR spoofing attacks. We envision three main directions for future research.

1. Multispectral-Spoof database offers just the most basic spoofing attacks with printed photographs. More challenging spoofing attacks need to be created and evaluated, like 3D attacks, or image-level fusion of VIS and NIR images.
2. Multispectral systems appear to be more robust, but still not highly secure under NIR spoofing attacks. Examining different fusion strategies at different levels, fine-tuning the training of the systems, fine-tuning the operating frequencies of the NIR and VIS systems, and including spoofing attacks to train the fusion systems are some of the possible ways to improve the multispectral systems.
3. The set of spoofing countermeasures for these systems is very sparse. Several of the hardware-based anti-spoofing methods described in Sect. 2.1.3 could be readily employed for detecting spoofing attacks in NIR spectrum as well. Yet, they may still be classified as requiring additional hardware, because they operate at different wavelengths then the wavelengths used by Multispectral-Spoof database. In practice, only [3] has developed a fully software-based countermeasures for printed attacks to NIR and multispectral systems, but its efficiency to other databases and more challenging spoofing attacks is still to be tested.

8.3 Face Recognition Systems Under 3D Spoofing Attacks

It is repeatedly stated in the previous sections that an attacker can attempt to gain access through a 2D face recognition system (visual, near-infrared, or multispectral) simply by using printed photographs or recorded videos of valid users. It is also reported that most of these attack types devised until today can be successfully averted by using various anti-spoofing methods.

A substantial part of the work on spoofing detection capabilities for face is based on the flatness of the surface in front of the sensor during an attack. For instance, the motion analysis techniques detailed in Sect. 2.1.3 rely on the assumption of shape

difference between an actual face and a spoofing attack instrument such as a paper or a tablet computer in order to distinguish motion patterns of a real person from an attacker. In a similar fashion, 3D shape information either extracted from multiple-view images or acquired using a 3D sensor (Sect. 2.1.3) can be exploited to positively detect 2D attacks. For instance, in [73], 3D data captured with a low-cost sensor is utilized to locate the face in an image as well as to test its authenticity.

These types of methods that rely on the assumption of a planar surface that displays a face image in front of the sensor are ineffective in case of 3D facial mask attacks [74]. Although the advancements in 3D acquisition and manufacturing technologies make this kind of attacks as untroublesome as their 2D counterparts, there have not been many studies published addressing this issue. In this section, an overview of the existing work is presented for several kinds of 3D attacks, face recognition systems, and spoofing countermeasures.

8.3.1 Types of Attacks and Databases

The earliest research works that target 3D attacks only aim to distinguish between facial skin and mask materials without analyzing the spoofing performances of the masks because they approach this problem as in an evasion or disguise scenario [61, 62]. The masks utilized for the experiments are not necessarily replicas of valid users.

Claiming that fake, by its definition, is indistinguishable for human eyes and visual spectrum cannot be sufficient to detect the attacks, a small group of studies follow the footsteps of early pioneers and propose multispectral analyses [63, 75] for mask and real face classification. The experiments in [63] are done on directly mask materials. In [75], some face-like masks are produced, but they do not mimic any real person. Unfortunately, no public database has been made available for further investigation.

Recently, another line of research in 3D spoofing has emerged for which the attacks are realized with 3D printed masks of valid users. Firstly, Kose et al. published a series of studies [76–79] on 3D mask attacks for which a non-public database of 16 users is utilized. In order to construct this database that is called Morpho database, a 3D face model of each client is captured by a 3D laser scanner. It consists of 207 real access and 199 mask attack samples as both 2D images and 3D scans (Fig. 8.6a).

Morpho database did certainly bring on a significant breakthrough and momentum in 3D spoofing attack research. Still, it was lacking a very crucial characteristic that is publicness. Taking this shortcoming into account, Erdogmus et al. collected the first public spoofing database with facial masks, called 3D Mask Attack Database (3DMAD) [80] and published a couple of spoofing and countermeasure analyses on several face recognition systems [80, 81]. The database contains 76500 real access and mask attack frames of 17 users, recorded using Microsoft Kinect.

Fig. 8.6 **a** Example shots from Morpho: The top row shows a real access from a user in *grayscale* texture (2D), depth map (2.5D), and 3D model format, while an attacker wearing the same users mask is displayed in the *bottom*. **b** Example papercraft mask from 3DMAD. **c** 17 Wearable resin masks from 3DMAD [81]

The masks used for Morpho database were printed using 3D laser scans of valid users. The acquisition process with such scanners requires cooperation since it is very sensitive movement and has range limitations. This makes the attack scenario less realistic. On the other hand, the masks for 3DMAD are manufactured using only 2D images of users via a private company which is specialized in facial reconstruction and in transforming 2D portraiture into 3D sculptures. Using this service, it is possible to construct a 3D face model from frontal and profile images of a person which can be easily obtained from a distance or found on the Internet. Once the 3D models are constructed, they can be turned into masks of various sizes and materials.

For 3DMAD, a life-size wearable mask and a papercraft mask are manufactured for each user (Fig. 8.6b, c). Papercraft masks can be just printed out and hand-crafted, so they are not recorded but made available within the database for the use of the biometrics community. Using Microsoft Kinect for Xbox 360, videos are recorded for real accesses and attacks with wearable hard resin masks. Since Kinect can capture both color and depth data, the database enables researchers to analyze the vulnerability of 3D face recognition systems to mask attacks and to devise countermeasures in 3D.

The two above-mentioned databases constitute the backbone of research on 3D spoofing attacks that investigate the ability of masks to spoof face recognition systems and the possible anti-spoofing techniques which will be detailed in the following subsections.

8.3.2 System Vulnerabilities

With both Morpho database and 3DMAD, vulnerabilities against spoofing with 3D masks have been analyzed extensively for 2D, 2.5D, and 3D face recognition systems.

In [79], a 2D system based on LBP and a 3D system based on thin plate spline (TPS) warping are analyzed for their robustness against mask attacks using the

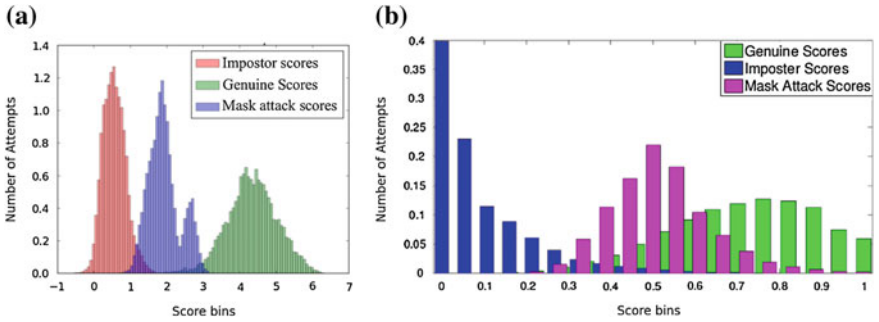

Fig. 8.7 Score distributions of genuine and impostor scores on the development set and mask attack scores on the test set of 3DMAD using **a** ISV [80]. **b** SRC [40], for 2D face verification

Morpho database. While both system performances decline remarkably as the attacks are introduced, 3D face recognition system which is completely based on 3D facial shape analysis is found to be affected more (EER increases from 1.8 to 25.1 %) than the 2D system (EER increases from 4.7 to 9.3 %). This is an expected outcome since the masks in Morpho database are highly precise in shape but have only grayscale texture. These findings are revised and extended in [77] with the addition of an LBP-based 2.5D face recognition system for which the EER increase from 7.27 % in normal mode to 14.26 % under spoofing attacks.

Similarly, 3DMAD is also assessed with regard to its spoofing ability on various face recognition systems. Firstly in [80], an inter-session variability (ISV)-based 2D face recognition algorithm is tried and 65.7 % of the mask attacks are found to be successful at EER threshold calculated on the development set of the database. The FAR at the same threshold would increase from 1.06 to 13.99 % if mask attacks are included in the probe partition together with the zero-effort impostors. The score distribution of the real access, zero-effort ,and mask attack impostors are given in Fig. 8.7a. The authors extend their study in [81] to include an ISV-based 2.5D and an Iterative Closest Point (ICP)-based 3D face recognition systems as well as all three baseline systems in [77]. Furthermore, spoofing performances are measured and reported separately for each mask. The experimental results reveal that the spoofing performances differ greatly not only between masks but also between modes and algorithms. Additionally, it is observed that the vulnerability to mask attacks is greater for more successful face verification algorithms that can generalize well to variations in facial appearance.

In a more recent work [82], 3DMAD masks are tested against another 2D face recognition algorithm which is based on the sparse representation classifier (SRC) and 84.12 % of the masks are found to be able to access the system at EER threshold (Fig. 8.7b).

All these findings expose that 3D mask attacks can be a real threat to all types of face recognition systems in 2D, 2.5D, or 3D and serious measures should be taken in order to detect and prevent them.

8.3.3 Spoofing CounterMeasures

Several methods have been proposed to detect 3D mask attacks in both 2D and 2.5D, mainly focusing on differences between micro-texture properties of mask materials and facial skin.

In [76], Kose et al. report 88.1 and 86.0 % accuracies on Morpho database with texture images (2D) and depth maps (2.5D), respectively, by concatenating histograms of different types of LBP and classifying them with an SVM classifier. Later in [79], they also try to fuse the two modes (image and depth map) at both feature and score level and reach 93.5 % accuracy. Other than micro-texture analysis via LBP, they also experiment with reflectance analysis to detect 3D mask attacks in [78] and report 94.47 % classification success. Finally, by fusing micro-texture and reflectance analyses in both 2D and 2.5D, an accuracy of 98.99 % is reached [83].

Spoofing countermeasure studies with 3DMAD also mainly revolves around LBP-based classification algorithms. In [80], the effectiveness of LBP-based features extracted from color and depth images to detect the mask attacks is analyzed. The results suggest that LBP features extracted from overlapping blocks give better results which achieve HTER of 0.95 and 1.27 % with images and depth maps separately. This study is elaborated further in [81] with best performance obtained by regular block-based LBP and a linear discriminant analysis (LDA) classifier at 0.12 ∓ 0.47 % and 3.91 ∓ 6.04 % HTER for 2D and 2.5D.

In addition to LBP, Raghavendra et al. propose to utilize binarized statistical image features (BSIF) to capture prominent micro-texture features [82] in 2D images both for the whole face (global) and the periocular (local) region. The LBP and BSIF features for each region are classified and the final scores are fused by weighted voting which results in an HTER of 4.78 %. Later in [84], the same protocol is also applied for 2.5D and the findings are incorporated via weighted score fusion. This addition is reported to push the HTER down to 0.03 %.

8.3.4 Discussion

Utilization of 3D masks for face spoofing has certainly become easier and cheaper. Many recent studies mentioned above have revealed the vulnerability of 2D, 2.5D, and 3D face recognition systems to such attacks. Additionally, many countermeasures have been proposed. However, as shown in [81], even though they are manufactured in similar ways, masks can behave very differently in various settings, making it very difficult to find one single solution that works for all.

Furthermore, in each of currently existing work, mask attack samples are utilized for training the anti-spoofing systems. This is not a realistic assumption for a biometric system since it cannot employ a different anti-spoofing module for each different mask. Worse still, it is always possible to encounter new and unseen types of masks.

Table 8.4 Categorization of anti-spoofing methods and overview of their main properties

Category	Method	Other category	Tested on public data	Source code	Intrusive	Type of input	Targeted attacks
Liveness detection	[28]	-	No	No	Somewhat	Video	Print
	[29]	-	No	No	Yes	Video	Print
	[30]	Motion analysis/fusion	No	No	Somewhat	Video	Print
	[31]	Visual appearance and motion analysis	Replay-Attack, CASIA-FASD	No	No	Video	All attacks
Motion analysis	[33]	-	No	No	No	Video	Print
	[34]	-	No	No	No	Video	Print/warped print
	[12]	-	Print-Attack	Yes	No	Video	Scenic print
	[13]	-	Photo-Attack	Yes	No	Video	Scenic print/photo
Visual	[38]	-	No	No	No	Video	Print
	[8]	-	NUAA	No	No	Image	Print
	[9]	-	CASIA-FASD	No	No	Image/video	Print/deformed print/video
	[42]	-	No	No	No	Image	Print
	[43]	-	No	No	No	Image	Print
	[45]	Fusion	Print-Attack	No	No	Image/video	Print
	[44]	-	NUAA, Print-Attack	No	No	Image	Print
	[46]	-	Replay-Attack	No	No	Image	Print/photo/video
	[48]	-	NUAA	No	No	Image	Print

(continued)

Table 8.4 (continued)

Category	Method	Other category	Tested on public data	Source code	Intrusive	Type of input	Targeted attacks
Appearance	[39]	Fusion	NUAA, Yale recaptured, Print-Attack	No	No	Image	Print
	[10]	-	Replay-Attack, NUAA, CASIA-FASD	Yes	No	Image	Print, photo, Video
	[37]	-	NUAA, Print-Attack, CASIA-FASD	Yes	No	Image	Print, Video
	[40]	-	No	No	No	Video	Print/Video
	[49]	-	Replay-Attack, CASIA-FASD	Yes	No	Video	Print, photo, Video
	[76]	-	-	No	No	Image	Mask
	[78]	-	Private database	No	No	Image	Mask
	[81]	-	3DMAD	Yes	No	Image	Mask
	[82]	Fusion	3DMAD	No	No	Image	Mask
Contextual	[7]	Liveness detection/fusion	No	No	Somewhat	Video	Scenic print/deformed print
Information	[51]	-	Yes	No	No	Image/video	Attacks with visible medium borders
3D information	[53]	Challenge response	No	No	Yes	Image sequence/video	2D attacks
	[54]	Challenge response	No	No	Yes	Video	2D attacks
	[55]	-	No	No	No	2 images	2D attacks
	[76]	-	-	No	No	Depth image	Mask
	[81]	-	3DMAD	Yes	No	Depth image	Mask
	[82]	Fusion	3DMAD	No	No	Depth image	Mask

(continued)

Table 8.4 (continued)

Category	Method	Other category	Tested on public data	Source code	Intrusive	Type of input	Targeted attacks
Challenge-	[56]	Motion analysis	No	No	Yes	-	-
Response	[57]	Motion analysis	No	No	Yes	Video	Print
Feature	[60]	-	Replay-Attack, CASIA-FASD	No	No	Image	All
Learning	[59]	-	Replay-Attack, 3DMAD	No	No	Image	All
Fusion	[11] [35]	Motion analysis/visual appearance -	Print-Attack Replay-Attack	No Yes	No No	Video Video	Print Scenic attacks

The anti-spoofing methods targeting 3D masks have been added to Table 8.4, together with the anti-spoofing methods for 2D attacks described in Sect. 8.2.1.3. Table 8.4 thus represents a comprehensive summarization of all the efforts in face spoofing detection in the visual spectrum that have been published so far.

8.4 Conclusions

Spoofing attacks are one of the most important reasons why face recognition may have a limited application in conditions where supervision is not possible. Face spoofing attacks have been proved to be effective for face recognition systems in visual spectrum in many occasions, including several face spoofing databases. So far, many countermeasures have been developed, and each of them tackles the problem from a different perspective. As a result, most of these countermeasures are effective just for a subset of the spoofing attack types. Having in mind the limitation of the currently available databases, as well as the possibility of new spoofing attacks appearing in future, more research efforts are needed to enhance the generalization capabilities of the countermeasures.

The work in spoofing face recognition systems in NIR is not as extensive. However, the newly developed Multispectral-Spoof database, which includes VIS and NIR attacks, demonstrates the vulnerability of both VIS and NIR systems to such attacks. Employing these systems in multispectral scenario significantly reduces the risks. Yet, development of suitable countermeasures is needed to provide acceptable security levels for multispectral face recognition systems.

The published research in anti-spoofing for face recognition rarely comes with data or source code that can be reproduced. This poses difficulties when comparing the performance of countermeasures. We would like emphasize the importance of publishing fully reproducible spoofing databases and countermeasures, as this will be of great benefit for building upon existing solutions and development to encourage the practice of new ones. In this chapter, we explicitly pointed out to solutions which are fully reproducible and we would like to encourage this practice for the future work.

References

1. Flynn, P.J., Faltemier, T., Bowyer, K.W.: 3D face recognition. In: Jain A.K., Flynn P., Ross A. A. (eds.) Handbook of Biometrics, pp. 293–313 (2008)
2. Socolinsky, D.A.: Multispectral face recognition. In: Jain A.K., Flynn P., Ross A.A. (eds.) Handbook of Biometrics, pp. 293–313 (2008)
3. Yi, D., Lei, Z., Zhang, Z., Li, S.: Face anti-spoofing: Multi-spectral approach. In: Marcel, S., Nixon, M.S., Li, S.Z. (eds.) Handbook of Biometric Anti-Spoofing, Advances in Computer Vision and Pattern Recognition, pp. 83–102. Springer, London (2014)
4. Duc, N.M., Minh, B.Q.: Your face is not your password. Black Hat Conference (2009)

5. Thalheim, L., Krissler, J., Ziegler, P.M.: Body check: Biometric access protection devices and their programs put to test. Heise Online (2002)
6. Chingovska, I., et al.: The 2nd competition on counter measures to 2D face spoofing attacks. In: International Conference of Biometrics (ICB) (2013)
7. Pan, G., Sun, L., Wu, Z., Wang, Y.: Monocular camera-based face liveness detection by combining eyeblink and scene context. Telecommun. Syst. **47**(3–4), 215–225 (2011)
8. Tan, X., et al.: Face liveness detection from a single image with sparse low rank bilinear discriminative model. ECCV **6**, 504–517 (2010)
9. Zhiwei, Z., et al.: A face antispoofing database with diverse attacks. In: Proceedings of the 5th IAPR International Conference on Biometrics (ICB'12), New Delhi, India (2012)
10. Chingovska, I., Anjos, A., Marcel, S.: On the effectiveness of local binary patterns in face anti-spoofing. In: Proceedings of the 11th International Conference of the Biometrics Special Interes Group (2012)
11. Komulainen, J., Anjos, A., Hadid, A., Pietikainen, M., Marcel, S.: Complementary counter-measures for detecting scenic face spoofing attacks (2013)
12. Anjos, A., Marcel, S.: Counter-measures to photo attacks in face recognition: a public database and a baseline. In: International Joint Conference on Biometrics 2011 (2011)
13. Anjos, A., Chakka, M.M., Marcel, S.: Motion-based counter-measures to photo attacks in face recognition. Inst. Eng. Technol. J. Biometrics (2013)
14. Chingovska, I., Anjos, A., Marcel, S.: Biometrics evaluation under spoofing attacks. IEEE Trans. Inf. Forensics Secur. **9**(12), 2264–2276 (2014)
15. Mansfield, A.J., Wayman, J.L.: Best practices in testing and reporting performance (2002)
16. Jain, A.K., Ross, A.: Handbook of Biometrics, chap. Introduction to Biometrics. Springer, Berlin (2008)
17. Cardinaux, F., Sanderson, C., Marcel, S.: Comparison of MLP and GMM classifiers for face verification on XM2VTS. In: Proceedings of the 4th International Conference on AVBPA. University of Surrey, Guildford, UK (2003)
18. Zhang, W., et al.: Local Gabor binary pattern histogram sequence (lgbphs): A novel non-statistical model for face representation and recognition. In: Proceedings of the Tenth IEEE International Conference on Computer Vision (ICCV'05) Volume 1—Volume 01, ICCV'05, pp. 786–791. IEEE Computer Society (2005)
19. Günther, M., Haufe, D., Wu¨rtz, R.P.: Face recognition with disparity corrected Gabor phase differences. In: Artificial Neural Networks and Machine Learning, *Lecture Notes in Computer Science*, vol. 7552, pp. 411–418. Springer Berlin (2012)
20. Wallace, R., McLaren, M., McCool, C., Marcel, S.: Inter-session variability modelling and joint factor analysis for face authentication. In: International Joint Conference on Biometrics (2011)
21. Schuckers, S.: Encyclopedia of Biometrics, chap. Liveness Detection: Fingerprint, pp. 924–931. Springer, Berlin (2009)
22. Ross, A., Nandakumar, K., Jain, A.K.: Handbook of Biometrics, chap. Introduction to multi-biometrics. Springer, Berlin (2008)
23. Akhtar, Z., Fumera, G., Marcialis, G.L., Roli, F.: Evaluation of serial and parallel multibiometric systems under spoofing attacks. In: 5th IEEE International Conference on Biometrics: Theory, Applications and Systems (2012)
24. Johnson, P.A., Tan, B., Schuckers, S.: Multimodal fusion vulnerability to non-zero (spoof) imposters. In: IEEE International Workshop on Information Forensics and Security (2010)
25. Rodrigues, R., Kamat, N., Govindaraju, V.: Evaluation of biometric spoofing in a multimodal system. In: Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on (2010)
26. Rodrigues, R.N., Ling, L.L., Govindaraju, V.: Robustness of multimodal biometric fusion methods against spoofing attacks. J. Vis. Lang. Comput. **20**(3), 169–179 (2009)
27. Chetty, G., Wagner, M.: Audio-visual multimodal fusion for biometric person authentication and liveness verification. In: Proceedings of the 2005 NICTA-HCSNet Multimodal User Interaction Workshop—Volume 57, pp. 17–24. Australian Computer Society, Inc. (2006)

28. Pan, G., Sun, L., Wu, Z., Lao, S.: Eyeblink-based anti-spoofing in face recognition from a generic webcamera. In: Computer Vision, 2007. ICCV 2007. IEEE 11th International Conference on, pp. 1–8 (2007)
29. Wang, L., Ding, X., Fang, C.: Face live detection method based on physiological motion analysis. Tsinghua Sci. Technol. **14**(6), 685–690 (2009)
30. Kollreider, K., Fronthaler, H., Bigun, J.: Verifying liveness by multiple experts in face biometrics. In: Computer Vision and Pattern Recognition Workshops, 2008. CVPRW'08. IEEE Computer Society Conference on, pp. 1–6 (2008)
31. Bharadwaj, S., Dhamecha, T., Vatsa, M., Singh, R.: Computationally efficient face spoofing detection with motion magnification. In: Computer Vision and Pattern Recognition Workshops (CVPRW), 2013 IEEE Conference on, pp. 105–110 (2013)
32. Wu, H.Y., Rubinstein, M., Shih, E., Guttag, J., Durand, F., Freeman, W.T.: Eulerian video magnification for revealing subtle changes in the world. ACM Trans. Graph. (Proceedings SIGGRAPH 2012) **31**(4) (2012)
33. Kollreider, K., Fronthaler, H., Bigun, J.: Non-intrusive liveness detection by face images. Image Vis. Comput. **27**(3), 233–244 (2009)
34. Bao, W., Li, H., Li, N., Jiang, W.: A liveness detection method for face recognition based on optical flow field. 2009 International Conference on Image Analysis and Signal Processing pp. 223–236 (2009)
35. Yan, J., Zhang, Z., Lei, Z., Yi, D., Li, S.Z.: Face liveness detection by exploring multiple scenic clues. In: 12th International Conference on Control, Automation, robotics and Vision (ICARCV 2012). China (2012)
36. Parziale, G., Dittman, J., Tistarelli, M.: Analysis and evaluation of alternatives and advanced solutions for system elements. BioSecure D 9.1.2 (2005)
37. Yang, J., Lei, Z., Liao, S., Li, S.: Face liveness detection with component dependent descriptor. In: Biometrics (ICB), 2013 International Conference on, pp. 1–6 (2013)
38. Li, J., et al.: Live face detection based on the analysis of Fourier spectra. Biometric Technology for Human Identification (2004)
39. Määttä, J., Hadid, A., Pietikäinen, M.: Face spoofing detection from single images using texture and local shape analysis. IET Biometrics **1**, 3–10 (2012)
40. Pinto, A.d.S., Pedrini, H., Schwartz, W.R., Rocha, A.: Video-based face spoofing detection through visual rhythm analysis. In: 25th Conference on Graphics, Patterns and Images (2012)
41. Oren, M., Nayar, S.K.: Generalization of the Lambertian model and implications for machine vision. International Journal of Computer Vision **14**(3), 227–251 (1995)
42. Bai, J., et al.: Is physics-based liveness detection truly possible with a single image? In: IEEE International Symposium on Circuits and Systems (ISCAS) (2010)
43. Gao, X., Ng, T.T., Bo, Q., Chang, S.F.: Single-view recaptured image detection based on physics-based features. In: IEEE International Conference on Multimedia & Expo (ICME) (2010)
44. Schwartz, W.R., Rocha, A., Pedrini, H.: Face Spoofing Detection through Partial Least Squares and Low-Level Descriptors. In: International Joint Conference on Biometrics (2011)
45. Tronci, R., et al.: Fusion of multiple clues for photo-attack detection in face recognition systems. In: IJCB, pp. 1–6 (2011)
46. Galbally, J., Marcel, S., Fierrez, J.: Image quality assessment for fake biometric detection: application to iris, fingerprint and face recognition. IEEE Trans. on Image Proc. **23**(2), 710–724 (2014)
47. Ojala, T., Pietikainen, M., Maenpaa, T.: Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE Trans. on Pattern Anal. and Mach. Intell. **24**(7), 971–987 (2002)
48. Määttä, J., Hadid, A., Pietikäinen, M.: Face spoofing detection from single images using micro-texture analysis. In: International Joint Conference on Biometrics, pp. 1–7 (2011)
49. de Freitas Pereira, T., et al.: Face liveness detection using dynamic texture. EURASIP J Image and Video Proc. **2014**:**2** (2014)

50. Zhao, G., Pietika¨inen, M.: Dynamic texture recognition using local binary patterns with an application to facial expressions. IEEE Trans. Pattern Anal. Mach. Intell. **29**(6), 915–928 (2007)
51. Komulainen, J., Hadid, A., Pietikainen, M.: Context based face anti-spoofing. In: Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on, pp. 1–8 (2013)
52. Dalal, N., Triggs, B.: Histograms of oriented gradients for human detection. In: Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on, vol. 1, pp. 886–893 (2005)
53. Wang, T., Yang, J., Lei, Z., Liao, S., Li, S.Z.: Face liveness detection using 3D structure recovered from a single camera. In: Biometrics (ICB), 2013 International Conference on (2013)
54. De Marsico, M., Nappi, M., Riccio, D., Dugelay, J.: Moving face spoofing detection via 3D projective invariants. In: Biometrics (ICB), 2012 5th IAPR International Conference on (2012)
55. Kim, S., Yu, S., Kim, K., Ban, Y., Lee, S.: Face liveness detection using variable focusing. In: Biometrics (ICB), 2013 International Conference on (2013)
56. Frischholz, R., Werner, A.: Avoiding replay-attacks in a face recognition system using head-pose estimation. In: Analysis and Modeling of Faces and Gestures, 2003. AMFG 2003. IEEE International Workshop on (2003)
57. Ali, A., Deravi, F., Hoque, S.: Spoofing attempt detection using gaze colocation. In: Biometrics Special Interest Group (BIOSIG), 2013 International Conference of the. IEEE (2013)
58. Chetty, G., Wagner, M.: Multi-level liveness verification for face-voice biometric authentication. In: Biometrics Symposium 2006 (2006)
59. Menotti, D., Chiachia, G., Pinto, A., Schwartz, W., Pedrini, H., Falcao, A., Rocha, A.: Deep representations for iris, face, and fingerprint spoofing detection. Inf. Forensics and Sec., IEEE Trans. on **99**, 1 (2015)
60. Yang, J., Lei, Z., Li, S.Z.: Learn convolutional neural network for face anti-spoofing. CoRR **abs/1408.5601** (2014)
61. Prokoski, F.J.: Disguise detection and identification using infrared imagery. pp. 27–31 (1983)
62. Pavlidis, I., Symosek, P.: The imaging issue in an automatic face/disguise detection system. In: Computer Vision Beyond the Visible Spectrum: Methods and Applications, 2000. Proceedings. IEEE Workshop on, pp. 15–24 (2000)
63. Kim, Y., Na, J., Yoon, S., Yi, J.: Masked fake face detection using radiance measurements. J. Opt. Soc. Am A **26**(4), 760–766 (2009)
64. Zhang, Z., Yi, D., Lei, Z., Li, S.Z.: Face liveness detection by learning multispectral reflectance distributions. pp. 436–441 (2011)
65. Wang, Y., Hao, X., Hou, Y., Guo, C.: A new multispectral method for face liveness detection. In: Pattern Recognition (ACPR), 2013 2nd IAPR Asian Conference on, pp. 922–926 (2013)
66. Angelopoulou, E.: Understanding the color of human skin. pp. 243–251 (2001)
67. Vink, J., Gritti, T., Hu, Y., de Haan, G.: Robust skin detection using multi-spectral illumination. In: Automatic Face Gesture Recognition and Workshops (FG 2011), 2011 IEEE International Conference on, pp. 448–455 (2011)
68. Raghavendra, R., Raja, K., Busch, C.: Presentation attack detection for face recognition using light field camera. Image Proc., IEEE Trans. on **99**, 1 (2015)
69. de Freitas Pereira, T., Anjos, A., De Martino, J.M., Marcel, S.: Can face anti-spoofing countermeasures work in a real world scenario? In: International Conference on Biometrics (2013)
70. Kuncheva, L.I., Whitaker, C.J.: Measures of diversity in classifier ensembles and their relationship with the ensemble accuracy. Mach. Learn. **51**(2), 181–207 (2003)
71. Li, S.Z., Chu, R., Liao, S., Zhang, L.: Illumination invariant face recognition using near infrared images. IEEE Trans. Pattern Anal. Mach. Intell. **29**(4), 627–639 (2007)
72. Zou, X., Kittler, J., Messer, K.: Ambient illumination variation removal by active Near-IR imaging. In: Zhang D., Jain A.K. (eds.) Advances in Biometrics, Lecture Notes in Computer Science, vol. 3832, pp. 19–25 (2005)

73. Tsalakanidou, F., Dimitriadis, C., Malassiotis, S.: A secure and privacy friendly 2D+3D face authentication system robust under pose and illumination variation. In: Image Analysis for Multimedia Interactive Services, 2007. WIAMIS'07. Eighth International Workshop on, pp. 40–40 (2007)
74. Erdogmus, N., Marcel, S.: Spoofing 2D face recognition systems with 3d masks. In: International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1–8 (2013)
75. Zhang, Z., Yi, D., Lei, Z., Li, S.Z.: Face liveness detection by learning multispectral reflectance distributions. In: IEEE International Conference on Automatic Face & Gesture Recognition and Workshops (FG), pp. 436–441. IEEE (2011)
76. Kose, N., Dugelay, J.L.: Countermeasure for the protection of face recognition systems against mask attacks. In: International Conference and Workshops on Automatic Face and Gesture Recognition (FG), pp. 1–6. IEEE (2013)
77. Kose, N., Dugelay, J.L.: On the vulnerability of face recognition systems to spoofing mask attacks. In: IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 2357–2361. IEEE (2013)
78. Kose, N., Dugelay, J.L.: Reflectance analysis based countermeasure technique to detect face mask attacks. In: International Conference on Digital Signal Processing (DSP), pp. 1–6. IEEE (2013)
79. Kose, N., Dugelay, J.L.: Shape and texture based countermeasure to protect face recognition systems against mask attacks. In: IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 111–116. IEEE (2013)
80. Erdogmus, N., Marcel, S.: Spoofing in 2D face recognition with 3D masks and anti-spoofing with kinect. In: International Conference on Biometrics: Theory, Applications and Systems (BTAS), pp. 1–6. IEEE (2013)
81. Erdogmus, N., Marcel, S.: Spoofing face recognition with 3D masks. IEEE Trans. Inf. Forensics Secur. **9**(7), 1084–1097 (2014)
82. Raghavendra, R., Busch, C.: Novel presentation attack detection algorithm for face recognition system: Application to 3D face mask attack. In: International Conference on Image Processing (ICIP), pp. 323–327. IEEE (2014)
83. Kose, N., Dugelay, J.L.: Mask spoofing in face recognition and countermeasures. Image Vis. Comput. **32**(10), 779–789 (2014)
84. Raghavendra, R., Busch, C.: Robust 2d/3d face mask presentation attack detection scheme by exploring multiple features and comparison score level fusion. In: International Conference on Information Fusion (FUSION), pp. 1–7. IEEE (2014)