Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey

RAGHAVENDRA RAMACHANDRA and CHRISTOPH BUSCH, Norwegian Biometric Laboratory, Norwegian University of Science and Technology (NTNU), Gjøvik, Norway

The vulnerability of face recognition systems to presentation attacks (also known as direct attacks or spoof attacks) has received a great deal of interest from the biometric community. The rapid evolution of face recognition systems into real-time applications has raised new concerns about their ability to resist presentation attacks, particularly in unattended application scenarios such as automated border control. The goal of a presentation attack is to subvert the face recognition system by presenting a facial biometric artifact. Popular face biometric artifacts include a printed photo, the electronic display of a facial photo, replaying video using an electronic display, and 3D face masks. These have demonstrated a high security risk for state-of-the-art face recognition systems. However, several presentation attack detection (PAD) algorithms (also known as countermeasures or antispoofing methods) have been proposed that can automatically detect and mitigate such targeted attacks. The goal of this survey is to present a systematic overview of the existing work on face presentation attack detection that has been carried out. This paper describes the various aspects of face presentation attacks, including different types of face artifacts, state-of-the-art PAD algorithms and an overview of the respective research labs working in this domain, vulnerability assessments and performance evaluation metrics, the outcomes of competitions, the availability of public databases for benchmarking new PAD algorithms in a reproducible manner, and finally a summary of the relevant international standardization in this field. Furthermore, we discuss the open challenges and future work that need to be addressed in this evolving field of biometrics.

Categories and Subject Descriptors: C.2.2 [**Pattern Recognition**]: Applications

General Terms: Design, Algorithms, Performance

Additional Key Words and Phrases: Biometrics, face recognition, antispoofing, security, attacks, countermeasure

ACM Reference Format:
Raghavendra Ramachandra and Christoph Busch. 2017. Presentation attack detection methods for face recognition systems: A comprehensive survey. ACM Comput. Surv. 50, 1, Article 8 (March 2017), 37 pages.
DOI: http://dx.doi.org/10.1145/3038924

1. INTRODUCTION

Biometric technology is rapidly gaining popularity and has become a part of our everyday lives. The goal of a biometric system is to automatically recognize individuals based on their biological and/or behavioural characteristics. Due to the nature of automatic processing, and also for the capture process, the extent of human supervision should be minimized and system components should enable the unsupervised capture of biometric data. Biometric systems can be constructed observing one or more biometric

This work was carried out with funding from the Research Council of Norway (Grant No. IKTPLUSS 248030/O70) and partial support from SECUNET Security Network AG, Germany.
Authors' addresses: R. Ramachandra and C. Busch, Norwegian University of Science and Technology (NTNU), Department of Information Security and Communication Technology, Mail Box 191 NO-2815, Gjøvik, NORWAY; emails: {raghavendra.ramachandra, Christoph.busch}@ntnu.no.

ACM 0360-0300/2017/03-ART8 $15.00
DOI: http://dx.doi.org/10.1145/3038924

characteristics, such as the face, iris, fingerprint, voice, finger vein, key stroke, gait, and others. Among the biometric systems that are deployed in an operational context, the use of face biometrics has a prominent role due to its widespread use in international border control [PASS 2014]. The deployed systems are built on signal processing experience from the last 40 years, which has resulted in the improved accuracy and reliability of face recognition algorithms. This performance increase permits the use of face biometrics in further diverse applications, which include forensics and surveillance, physical and logical access control, and e-commerce and e-government contexts.

Following the specifications for electronic passports [International Civil Aviation Organization NTWG 2006] and the widespread deployment of these passports in the last 10 years, face recognition based on these passports has become a prominent application [PASS 2014]. In the context of border control, face recognition has the obvious advantage that the comparison can be conducted with visual evidence in a case of a false-negative decision by the system. Moreover, face recognition is associated with advantages such as nonintrusive data capture and low-cost sensors. Recent analysis forecasts that the global facial recognition market will reach $2.9 billion by 2019 [Market 2015]. These figures strongly indicate the popularity and the adoptability of face recognition systems for various applications both by government agencies and in the private sector.

The widespread appliance of face recognition systems has also raised new concerns, particularly regarding the vulnerability of the data capture subsystem and the overall system.[1] Spoofing is no longer restricted to Hollywood fantasy movies. Recently, a real case was reported in which a young person from Hong Kong boarded a plane to Canada disguised as an old man with a flat hat [Mail 2015]. This person used a silicon face and neck mask to successfully fool the border control authorities. In addition, the black hat test reported in Duc and Minh [2009] illustrates how to spoof face recognition systems available on laptops from different manufacturers. These cases illustrate the vulnerability of face recognition systems in the real world. The motivation for attackers is high, as an attack can be executed easily and the necessary facial artifacts can be created in a cost-effective manner. Furthermore, the information and video illustrations of how to create these face artifacts are provided on various web pages [Mask 2014]. Lastly, in facial biometrics, it is often easy to obtain an image of the face of the target individual either by searching on social network sites or by capturing their facial image in a nonintrusive manner over a long distance. These reference images are copied or captured without the target victim being aware of the attack. Such images may then be used to create face artifacts to fool the face recognition system. These factors have triggered various researchers to address the challenges of presentation attack detection for facial biometric systems.

Recently, the topic of presentation attack detection for face recognition systems has gained a great deal of interest among biometric researchers in both academia and industry. As a consequence, there is a considerable amount of literature available that can provide insight into both the vulnerability of data capture subsystems and presentation attack detection methods in face recognition systems [Hadid 2014; Galbally et al. 2014a], publicly available databases [Tan et al. 2010; Anjos and Marcel 2011; Chingovska et al. 2012; Zhang et al. 2012], dedicated books [Marcel et al. 2014], patents [Troy et al. 2014; Lindemann 2014; Dewan et al. 2013; Unnikrishnan 2014; Chaudhury and Devarasetty 2014; Rowe 2010; JUNG et al. 2010; Yamada and Yamaguchi 2010; Competition 2013], international standards [ISO/IEC JTC1 SC37 Biometrics 2016], and opensource software [Anjos et al. 2012; PRALAB 2010]. Furthermore, the

[1]Other biometric modalities are also vulnerable to presentation attacks, and interested readers can refer to Marcel et al. [2014] for more details.

European Union (Framework Program 7) has sponsored a number of research projects, namely, TABULA [RASA 2009], FASTPASS [PASS 2012]. and BEAT [2010] that have not only contributed to the creation of awareness of vulnerabilities but also proposed various algorithms to increase the robustness of facial recognition systems against different kinds of face artifacts. There is also a working group called the Biometric Vulnerability Assessment Expert Group (BVAEG) [BVAEG 2010] that encourages the face biometric vendors to incorporate antispoofing schemes. Unfortunately, there is little transparency in the work of this group. In view of the significance of this problem, many commercial face recognition vendors such as MORPHO [face 2010a], Cognitec [Cognitech 2010], NEC [face 2010b; KeyLemon 2012] and MODI [2015] provide face antispoofing functionality for photo and video attacks as components of their face recognition systems.

In this article, we present a comprehensive review of all pioneering efforts on facial presentation attack detection (PAD) algorithms. A couple of previous survey papers on face antispoofing can be found in the literature: the first example is Hadid [2014], which provides a brief overview of existing face antispoofing schemes and databases; the second is Galbally et al. [2014a], which presents an overview of existing antispoofing techniques along with information on the available face-spoofing databases, and which also provides information on general aspects of biometric antispoofing methods. Thus, both of these survey papers are focused specifically on discussing the different types of face artifacts, PAD (or countermeasure or antispoofing) schemes, and face-spoofing databases. However, these existing survey papers do not provide a common evaluation framework for analyzing the performance of the existing PAD algorithms, and they also lack a vulnerability analysis regarding commercial off-the-shelf (COTS) face recognition systems. By considering the rapid advancements in this field, this work contributes the following:

—A complete overview of recent research on face PAD techniques, publicly available databases, and the level of performance achieved by publicly organized competitions.
—Extensive analysis of 14 different state-of-the-art (SOTA) PAD techniques in a common evaluation framework.
—Extensive analysis on the vulnerability of the VeriLook face recognition system to three different face artifacts captured at various levels of image quality.
—A preliminary analysis of identical twins as a special case of face presentation attack.
—The provision of insights into the relevant international standards of PAD (ISO/IEC 30107-1:2016 [ISO/IEC JTC1 SC37 Biometrics 2016] and ISO/IEC DIS 30107-3 [International Organization for Standardization 2016]). The latter project was established to provide standardized metrics for evaluating the efficiency of face antispoofing mechanisms.

Overall, this article provides a review of the progress that has been achieved in the field of face antispoofing and thus can serve as a complete reference guide for both newcomers and experts working on the security evaluation of biometric systems.

The rest of the article is organized as follows: Section 2 presents the general concepts involved in the vulnerability of a face recognition system, Section 3 presents details of different types of face artifacts, and Section 4 presents and discusses the merits and drawbacks of existing presentation attack detection schemes. In Section 5, we provide an overview of all publicly available databases. Section 6 gives an overview of all face antispoofing competitions, Section 7 provides performance metrics according to ISO/IEC DIS 30107-3, and Section 8 presents the performance evaluation of 14 different static PAD techniques following a unifying framework. Section 9 presents the preliminary results on the identical twins as a possible presentation attack on the face

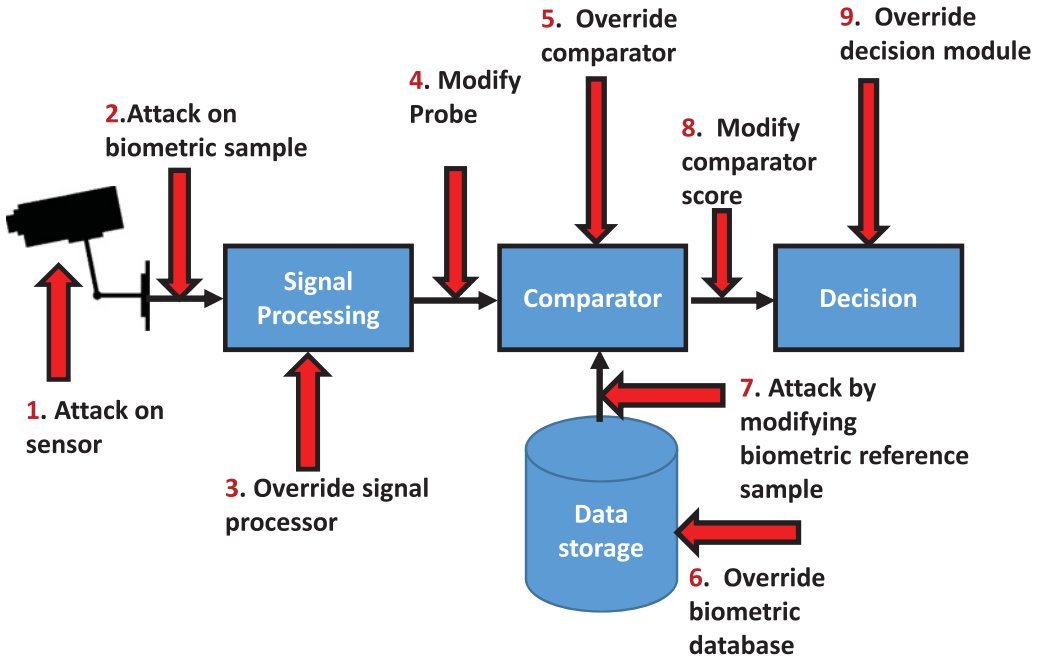

Fig. 1. Vulnerability of a face recognition system (inspired by figure in ISO/IEC 30107-1 [ISO/IEC JTC1 SC37 Biometrics 2016]).

recognition system. Section 10 delineates future perspectives and Section 11 presents the conclusion.

2. VULNERABILITIES OF FACE RECOGNITION SYSTEMS

Figure 1 shows a block diagram of a generic face recognition system with nine different vulnerabilities, as indicated in ISO/IEC 30107-1:2016 [ISO/IEC JTC1 SC37 Biometrics 2016]. The first vulnerability is noted at the sensor (i.e., the data capture subsystem) and involves presenting a face biometric artifact of the legitimate user as an input to the sensor. An artifact is defined in ISO/IEC JTC1 SC37 Biometrics [2016] as *an artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns*. This kind of attack is known as a presentation attack and is defined as *a presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system* [ISO/IEC JTC1 SC37 Biometrics 2016]. The second vulnerability is related to intercepting the biometric sample that was captured by the sensor. This attack basically involves replacing the captured face biometric sample with a fake sample. The third vulnerability is overriding the signal processing module. This could involve modifying the functionality of the feature extractor, for instance, using a Trojan horse. The fourth vulnerability allows the attacker to replace the extracted features of the probe sample with target features. The fifth vulnerability involves overriding the comparator so that it will output a comparison score required by the attacker. The sixth vulnerability involves replacing the reference template such that the authorized ID is associated with the attacker template. The seventh vulnerability is the modification of the reference template in the communication channel. The eighth vulnerability is the interception and corruption of the comparator output. Lastly, the ninth vulnerability involves overriding the decision module to output the intended decision. Of these nine vulnerabilities, only the first involves an

attack on the sensor itself; all the other vulnerabilities are related to the integrity of the overall system. Attacks on facial sensors have garnered wide interest from the biometric community, as using this approach, (1) it is easy to attack a biometric system, (2) it is easy to generate the face artifact and to present it to the sensor, and (3) it does not require knowledge about the operational details of the biometric system. Thus, in this article, we focus on presentation attacks at the sensor. However, readers can refer to Martinez-Diaz et al. [2011] to obtain more insight into indirect attacks and Frontex [2015] to gain information on the recommended security settings for deployed biometric systems [Frontex 2011].

Presentation attacks can be broadly classified into two types [ISO/IEC JTC1 SC37 Biometrics 2016]: (1) An active impostor presentation attack, in which the subversive data capture subject intends to be recognized as a different individual [ISO/IEC JTC1 SC37 Biometrics 2016]. This can in turn be one of two types of attack: in the first case, the subversive data subject intends to be recognized as a specific individual known to the system, while in the second case the aim is to be recognized as any other individual, without specification as to which. (2) A concealer presentation attack: in this case, the subversive data subject intends to evade being recognized as any individual known to the system [ISO/IEC JTC1 SC37 Biometrics 2016].

Thus, one can consider presentation attacks within both the verification and identification operating scenarios of biometric systems. For instance, a presentation attack can be carried out during authentication by presenting a biometric artifact of a legitimate user who is enrolled in the biometric system. For the case of an identification system (in an open set application), the attacker can conceal his or her identity by presenting disguised or altered biometric characteristics [John et al. 2014]. Thus, the presentation attack can be conducted on the biometric systems with the intent not only to gain access to the services attributed to a legitimate user but also to hide the attacker's identity from being revealed to the biometric systems.

3. FACE ARTIFACTS

According to ISO/IEC 30107-1, the *biometric characteristic or object used in a presentation attack* is termed the Presentation Attack Instrument (PAI) [ISO/IEC JTC1 SC37 Biometrics 2016]. The PAI can be broadly classified into two types: (1) *Artificial:* This refers to an artificial means of generating the PAI. This in turn can be classified as (a) *complete,* referring to the generation of a complete artificial PAI, for example, a video of a face, a 3D face mask, a 2D face print, and so forth, (b) *partial,* which involves an artificial PAI that can show partial biometric characteristics, for instance, a face video with sunglasses or a partially visible face. (2) *Human characteristics:* This involves using humans as a PAI and can be (a) *lifeless:* for instance, a cadaver part of the face; (b) *altered:* including the mutation of faces and cosmetic surgery; (c) *nonconformant:* this includes the use of facial expression(s); (d) *coerced:* this includes the use of the face of an unconscious human; or (e) *conformant:* this includes zero-effort impostor attempts. Of these different types of PAI, the artificial PAI is most widely used by research labs to study the vulnerabilities of face recognition systems.

Face artifacts can be easily generated simply by taking a photo of a legitimate user who is enrolled in the biometric system. Face artifacts are commonly generated using (1) a photo print with a laser jet printer [Anjos and Marcel 2011; Zhang et al. 2012; Raghavendra et al. 2015], (2) a photo print with an inkjet printer [Raghavendra et al. 2015], (3) an electronic display of a photo or video of a face [Zhang et al. 2012; Chakka et al. 2011; Raghavendra et al. 2015], or (4) a 3D face mask [Nesli and Marcel 2013] and (5) MakeUp [Cunjian et al. 2017].

Figure 2 shows examples of face artifacts that can be used to carry out a presentation attack on the target face recognition system. The goal is to distinguish attack

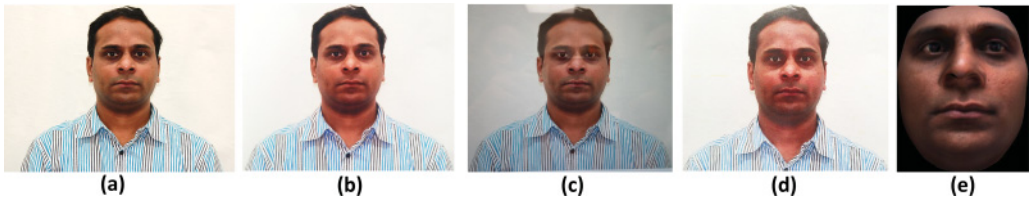

Fig. 2. (a) Bona fide facial image and examples of face artifacts: (b) laser print face artifact; (c) display face photo artifact using an iPad; (d) inkjet print face artifact; (e) 3D face mask.

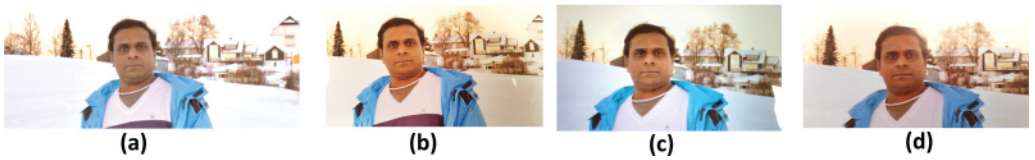

Fig. 3. Illustration of face artifacts generated using the legitimate user photo obtained from a social website: (a) photo from the social website, (b) inkjet print, (c) electronic display, and (d) laser print.

presentations from a bona fide presentation; these are defined as the *interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system*. Figure 2 shows (a) the real face image (captured from a bona fide presentation) of the legitimate user that was stored in the face recognition system. If we assume that the enrolled bona fide image (shown in Figure 2(a)) of the legitimate user is somehow leaked from the face data storage subsystem, and the attacker wants to use this leaked enrolled face image to generate a PAI, then the attacker can generate the face artifact by printing the leaked photo using a laser jet printer, as shown in Figure 2(b); by storing this hacked image in an electronic display (for instance, an iPad tablet device) and presenting this to the face recognition sensor, as shown in Figure 2(c); or by printing the photo of the legitimate user on an inkjet printer, as shown in Figure 2(d). Furthermore, the attacker can use a small set of photos from the legitimate user and create a 3D mask by uploading reference samples to a specialist Internet service [Mask 2014]. Figure 2(e) shows examples of 3D face masks that can be obtained from www.thatsmyface.com.

In the same way, the attacker can also easily find photos of legitimate users by visiting social media websites such as Facebook and Twitter and personal or professional webpages. Attackers can then use these photos to generate artifacts, as shown in Figure 3, which in turn can be used to perform a presentation attack on the face recognition system. Figure 3(a) shows a photo obtained by an attacker by visiting a social media website, Figure 3(b) shows a face artifact generated by printing the photo in Figure 3(a) using an inkjet printer, Figure 3(c) shows a face artifact generated using an electronic display (for instance, an iPad), and Figure 3(d) shows the face artifact generated by printing the photo in Figure 3(a) using a laser printer. This demonstrates the ease with which face artifacts can be generated.

The face artifacts shown in Figures 2 and 3 can also be used to perform a presentation attack on a face recognition system operating in either a verification or a closed identification scenario. However, in order to perform an identity concealer presentation attack on a face biometric system operating in an open identification scenario (or watchlist scenario), the attacker needs to disguise his or her facial characteristics. The ideal case for this kind of attack is using a 3D face mask, which was in fact exploited in a real forensic case mentioned in Mail [2015]. The use of 3D masks appears to be very efficient, if the face biometric system is operating under supervision and with the aid

Fig. 4. Examples of face disguise PAI (taken from IIITD face disguise database [Dhamecha et al. 2014]).

of human assistance. In case of an autonomous face recognition system, one can use additional low-cost PAIs to conceal the attacker's identity by presenting altered face characteristics.

Figure 4 shows disguised faces (i.e., PAIs), which can be used to perform a concealer presentation attack on a face recognition system operating in an open identification scenario. Face disguise recognition is well addressed in the literature [Dantcheva et al. 2012; Dhamecha et al. 2014]. These research results clearly indicate that it is difficult to recognize data subjects who present themselves with a disguise. The central idea of these attacks is to conceal the identity by changing the appearance, so that the capture subject will not be identified if he or she is included on a watch list. The face disguise attack can be performed easily, especially in automatic access control applications such as entry and exit control in football stadiums, restricted areas, and so on.

Presentation attacks on facial recognition systems using good-quality face artifacts always increase the criticality of the attack. However, the success of the attack also depends on the presentation skills of the attacker, since these require suitable poses or the rotation of the presentation attack instrument, especially when performing a handheld presentation attack. The vulnerability analysis of all four kinds of face artifacts, as shown in Figures 2 and 3, have been extensively studied in Chingovska et al. [2014] and Kose and Dugelay [2013b]. The analysis of the vulnerability will help to estimate the extent to which the face biometric system can be spoofed. The vulnerability can be measured using the metric of *spoof false accept rate* (SFAR) [Adler and Schuckers 2015],[2] which can be defined as the percentage of artifacts accepted by the recognition system.

Table I indicates the vulnerability of face recognition systems with respect to the video replay attack, the 3D mask attack, and the print attack. The vulnerability of the face recognition system depends on the baseline algorithm used. It is interesting to observe from Table I that irrespective of the baseline algorithm, the face recognition system is vulnerable to all four kinds of face artifact discussed in Section 3.

3.1. Vulnerability of the VeriLook Face Recognition System

To understand the influence of face artifacts on a real-life scenario, we evaluate the vulnerability of a commercial off-the-shelf (COTS) face recognition system. To this end, we investigate the VeriLook facial recognition system developed by Neurotech [COTS 2015]. The evaluation is carried out on the CASIA face-spoofing database [Zhang

[2]According to the recently developed standard ISO/IEC 30107-3, the concept of SFAR is now defined as the Imposter Attack Presentation Match Rate (IAPMR), which is, in a full-system evaluation of a verification system, the proportion of imposter attack presentations using the same PAI species in which the target reference is matched.

Table I. Vulnerability of Different Face Recognition Systems to Various Kinds of Face Artifacts Using the Metric of *Spoof False Accept Rate (SFAR)*

Database	Baseline Face Recognition Algorithm	SFAR (%)
IDIAP - Replay Attack DB [Chingovska et al. 2012]	Gaussian Mixture Models (GMMs) [Chingovska et al. 2014]	91.5
	Log-Gabor Binary Pattern Histogram (LGBPHS) [Chingovska et al. 2014]	88.5
	Gabor Jet [Chingovska et al. 2014]	95.0
	Intersession Variability (ISV) [Chingovska et al. 2014]	92.6
IDIAP-3D Mask Attack [Nesli and Marcel 2013]	Sparse Representation Classifier (SRC) [Raghavendra and Busch 2014a]	84.1
	Intersession Variability (ISV) [Nesli and Marcel 2013]	65.7
IDIAP-Print Attack DB [Anjos and Marcel 2011]	Gabor graph [Erdogmus and Marcel 2013]	78.3
	Log-Gabor Binary Pattern Histogram (LGBPHS) [Erdogmus and Marcel 2013]	97.5

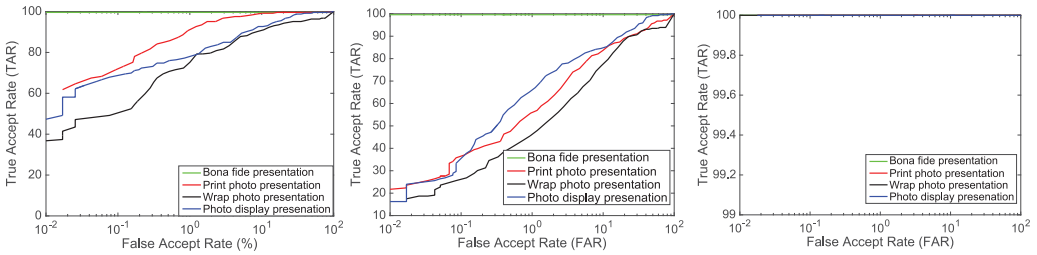

Fig. 5. Verification performance of a VeriLook face recognition system on the CASIA face-spoofing database with (a) low quality, (b) medium quality, and (c) high quality.

et al. 2012]. We selected this database since it has both bona fide and artifact face images recorded at three different qualities, that is, low, medium, and high quality. Furthermore, this database is also made up of three types of face artifacts: print photo, wrap photo, and photo display.

We performed the verification experiments by enrolling each subject with a real bona fide sample. As a probe, we are using both real and artifact face images from the CASIA face-spoofing database. Figure 5 shows the receiver operating characteristic curves (ROCs) [International Organization for Standardization 2006] indicating the performance of the VeriLook face recognition system for low-quality samples (see Figure 5(a)), medium-quality samples (see Figure 5(b)), and high-quality samples (see Figure 5(c)). It can be observed from the results that the VeriLook face recognition system is not capable of distinguishing between real and artifact face samples. The verification of this system for high-quality samples indicates a verification rate with a TAR of 100% at an FAR of 0.01%. This indicates a high vulnerability and the need for a presentation attack detection subsystem before the probe sample is submitted for facial comparison. It is also interesting to note the quality of the face images used to generate the face artifact. Our experiments indicate that using high-quality face samples with good resolution will give rise to a high vulnerability for the face recognition system. Additionally, it is also observed that the print photo attack is more effective in

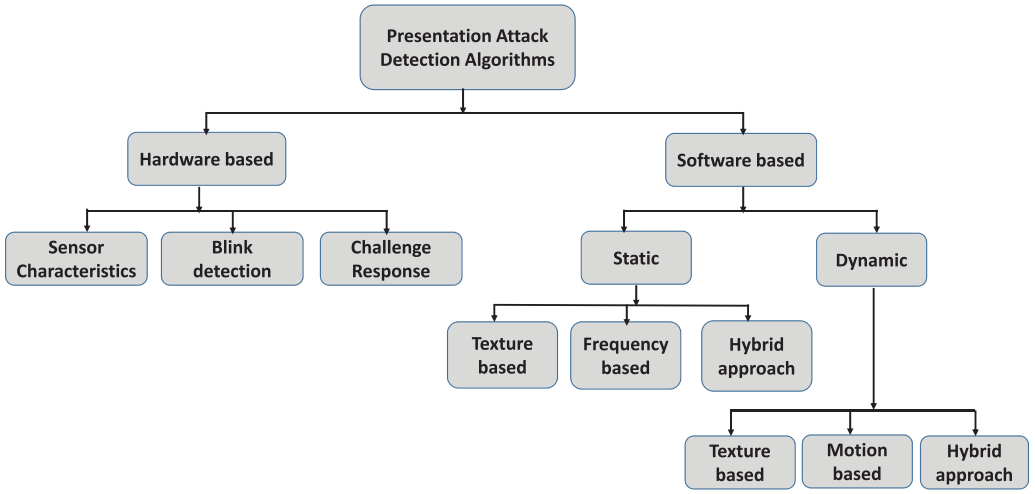

Fig. 6. Classification of face presentation attack detection (PAD) algorithms.

attacking the VeriLook face recognition system when compared with either the wrap photo or display (or electronic screen) photo attacks on the face recognition system irrespective of the image quality. For a more detailed analysis of the VeriLook face recognition system, especially in an identification scenario, readers can refer to Wen et al. [2015].

4. PRESENTATION ATTACK DETECTION METHODS

As discussed in the previos section, facial recognition systems are vulnerable to various kinds of artifacts (or PAIs) that can be generated cost-effectively. This demands a need to detect and mitigate these attacks in order to improve both the security and the reliability of face recognition systems. A PAD method can be defined as an *automated determination of a presentation attack* [ISO/IEC JTC1 SC37 Biometrics 2016]. In the literature, PAD is also referred to as a countermeasure or an antispoofing technique. In most of the existing works, PAD is also referred to as liveness detection; however, strictly speaking, liveness detection is defined as the *measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, in order to determine if a biometric sample is being captured from a living subject present at the point of capture* [ISO/IEC JTC1 SC37 Biometrics 2016]. Following this standardized definition of the term, liveness detection can be considered as a subset of PAD but not as a synonym for PAD itself.

Figure 6 shows the classification of existing face PAD algorithms. These existing algorithms can be broadly classified into two types, namely, (1) hardware based and (2) software based.

Hardware-Based PAD Techniques

Hardware-based approaches explore the characteristics of the human face using dedicated additional hardware components that work in association with the face recognition sensor. These approaches may also require an interaction with the hardware or a face capture sensor (such as eye blinking), which will also use software internally to process the captured face data. The hardware-based approaches can be broadly classified into three types: *sensor characteristics, blink detection,* and *challenge response*, all of which are described in detail as follows.

Fig. 7. Illustration of using a variation of focus rendered by the LFC to detect face artifacts: (a) real face focus images rendered by the LFC; (b) inkjet print attack focus images rendered by the LFC; (c) display attack using iPad focus images rendered by the LFC; and (d) laser print attack focus images rendered by the LFC.

Sensor Characteristics. The techniques developed in this approach are based on exploring the characteristics of the camera (or sensor) used to capture the face image (or video). The characteristics of the sensor explored depend on the type of sensor used to capture the face data, for example, measuring the variation of the focus with a light field camera (LFC) or measuring the reflectance from a near-infrared/thermal/multispectral face sensor or measuring the reflectance in a 3D scan. To illustrate the principle behind the PAD techniques developed in these sensor-based approaches, we consider the example of using a light field camera (LFC) as the face capture sensor [Raghavendra et al. 2015]. The light field camera records both the direction and the intensity of the incoming light rays, and thus the LFC can render multiple face images that can reflect the variation of depth (in terms of focus) in a single capture attempt. The LFC camera characteristic was explored in Raghavendra et al. [2015] with the ability to detect photo and display (or electronic screen) attacks. Figure 7 shows the results of this example on exploring the variation of focus on both real (Figure 7(a)) and face artifacts generated using a photo print (both inkjet (Figure 7(b)) and laser print (Figure 7(d))) and electronic display using an iPad (Figure 7(c)). As can be observed from Figure 7, the focus variation is relatively high for real images when compared with artifact images. This can be attributed to the fact that the bona fide subjects will exhibit more depth information when compared to the depth variation observed from artifacts.

Another interesting illustration is the use of a multispectral face sensor. Since this sensor will simultaneously capture both visible and near-infrared face images, the artifacts can be detected much more easily by processing color and texture information [Yi et al. 2014]. It is interesting to note from Figure 8 that the artifact type (including the presentation attack instrument species) plays a vital role in spoofing the multispectral face sensor. Figure 8(c) corresponds to a face artifact generated by printing the bona fide image onto high-quality glossy paper. The use of an inkjet printer results in a high-quality face artifact, and this works efficiently in the visible spectrum (see Figure 2(d)). However, it results in a very low-quality artifact when captured with a near-infrared sensor. The same observation can also be made for a photo print using a laser printer, as it indicates the dot patterns when captured in a near-infrared spectrum (see Figure 8(b)). A similar effect is also noted for a 3D mask (see Figure 8(e)) and for a

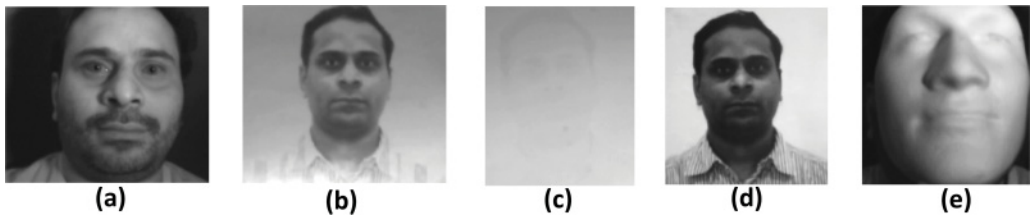

Fig. 8. Illustration of near-infrared face capture of (a) bona fide (real) face; (b) photo print using a laser printer; (c) photo print using an inkjet printer; (d) display attack using an iPad; and (e) 3D mask attack.

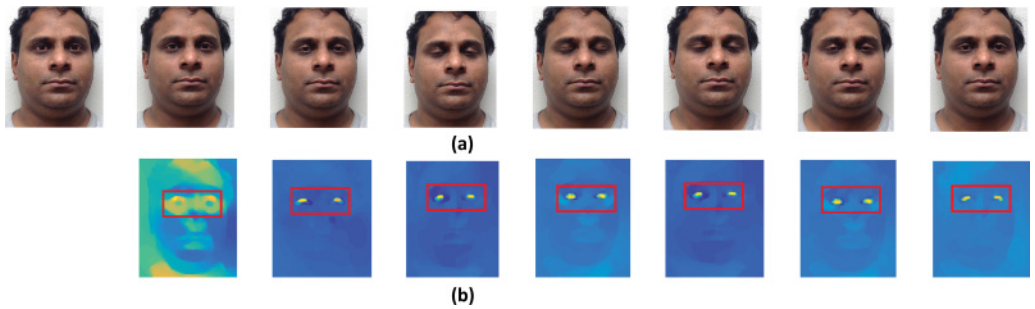

Fig. 9. Illustration of eye-blink detection as a face presentation attack detection mechanism: (a) video frames and (b) corresponding optical flow.

display attack using an iPad (see Figure 8(d)), which are captured in the near-infrared spectrum. Based on these qualitative illustrations, the use of multispectral light will help in detecting a presentation attack against a multispectral face recognition system by exploring complementary information. However, the systematic study reported in Chingovska et al. [2016] indicates the vulnerability of multispectral face recognition systems. Recently, the vulnerability of the extended multispectral face recognition system was explored for the first time in Raghavendra et al. [2017].

Blink Detection. Blink detection is a widely used liveness measure to mitigate presentation attacks against face recognition systems. The idea behind blink detection is to continuously track the spontaneous action of eye blinks that are performed unconsciously. Eye-blink detection can be carried out either using dedicated hardware [Hammoud 2008] or a software-based technique [Bhaskar et al. 2003; Hammoud 2008; Chrzan 2014; Gang et al. 2007].

Figure 9 illustrates the underlying concept of eye-blink detection: Figure 9(a) shows the video frames and Figure 9(b) the motion estimated using the optical flow [Liu 2009]. Since the eye region exhibits a larger motion due to eye blinking, a large magnitude of motion is observed in the eye region when compared with other regions in the face. This feature can be used to detect a presentation attack if the attacker presents face artifacts (e.g., a photo attack). However, it is well known in the biometric community that blink detection can be easily spoofed, either by wearing a shaped mask with the eye region open or by displaying a video replay to the face sensor. This fact is illustrated in Figure 10, where the attacker wears a mask of a legitimate user that contains open eye regions and presents himself to the face sensor. Figure 10(a) shows the recorded video frames, and Figure 10(b) shows the optical flow computed between frames to capture the motion in the eye region. Here it can also be observed that the use of a simple optical flow algorithm can capture the movement from the eye region due to the eye blinking,

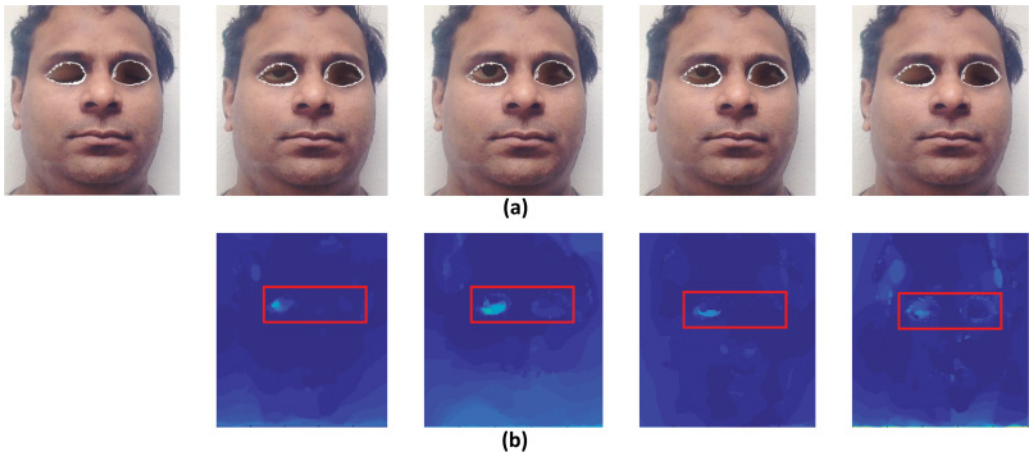

Fig. 10. Illustration of a presentation attack using a mask with eye region open in order to spoof blink detection: (a) video frames and (b) motion computed using optical flow.

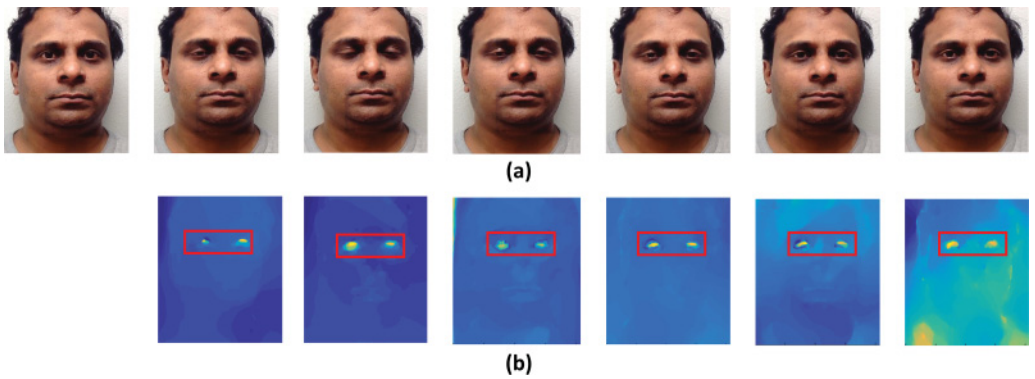

Fig. 11. Illustration of the use of blink detection on a video replay attack: (a) video replay attack frames and (2) optical frames.

as shown in Figure 10(b). This illustrates that even though the blink detection itself is robust, an attacker can still successfully perform a presentation attack.

Figure 11 illustrates the limitations of blink detection when a video replay attack is used together with the motion magnitude computed from optical flow.

Challenge Response. The idea behind challenge-response-based presentation attack detection is to provide a separate user interface in which the response to a challenge is recorded and processed to identify a bona fide presentation, for example, by tracking the gaze of the user toward a predefined stimulus [Ali et al. 2013].

Table II provides a general overview of different state-of-the-art (SOTA) approaches that fall under hardware-based face PAD methods. As can be noted from Table II, the selection of one approach over another is difficult. However, general opinion may prefer sensor-based characteristics (either the use of multispectral or light field camera) over one of the other two approaches based on blink detection and challenge response. This is because the latter two methods demand a high level of user cooperation; in addition, the performance is limited to the rather simple photo attack. Table III provides a summary of the advantages and limitations of hardware-based approaches.

Table II. Brief Overview of Hardware-Based PAD Techniques

Reference	Techniques	Attacks	Database
Raghavendra et al. [2015]	Variation of focus using light field camera	Photo attack & display (iPad)	Public, 80 subjects
Yi et al. [2014]	Color & texture using mutispectral light	Photo	Proprietary, 100 subjects
Zhang et al. [2011]	Reflectance using multispectral light	Photo, video replay, & 3D masks	Proprietary, 40 subjects
Gang et al. [2007]	Blink detection using conditional random fields (CRFs)	Photo	Proprietary, 20 subjects
Chrzan [2014]	Blink detection using optical flow	Photo	Proprietary, 20 subjects
Kollreider et al. [2008]	Challenge response and blink detection using motion	Photo, video replay	Proprietary, 15 subjects
Ali et al. [2013]	Challenge response using gaze collinearity	Photo	Proprietary, 8 subjects
Kose and Dugelay [2013c]	Reflectance measure	3D face mask	Proprietary, 20 subjects
Kim et al. [2015a]	Variance of the subregions in microlens of light field camera	Photo	Proprietary, 24 subjects
Smith et al. [2015]	Challenge response by displaying different colors on face	Photo & video replay	Proprietary, 10 subjects
Hou et al. [2013]	Multispectral gradient	Photo	Proprietary, 70 subjects
Lagorio et al. [2013]	3D face sensor	Photo	Proprietary, 70 subjects

Table III. Advantages and Limitations of Hardware-Based Approaches

Methods	**Advantages**	**Limitations**
Sensor characteristics	-Good generalizability	-Moderate computation cost -High sensor cost
Blink detection	-Effective for display photo attack	-Computation overhead -Not effective for video replay and mask attacks
Challenge response	-Generalizability (reasonably) -Effective for both photo and display attack	-High computation cost -User inconvenience -Not effective for replay video attacks -Dedicated hardware

The use of hardware-based methods may provide the desired accuracy for photo, display, and video replay attacks but will increase the cost as well as computational response of the existing face recognition system. This aspect has motivated biometric research labs to investigate so-called *software-based approaches* that are known to be cost-effective and easy to integrate with existing face recognition systems.

Software-Based PAD Techniques

Software-based approaches involve an algorithm that can determine whether a captured face sample stems from either an attack presentation or a bona fide presentation (also known as a real or live presentation). This kind of PAD scheme has been demonstrated to have high accuracy and relatively low cost. Moreover, these schemes do not require user cooperation and also obviate the need for specialized hardware. The existing methods in this family can be further divided into two main types: (1) static methods and (2) dynamic methods.

Static Approaches. The static approaches are designed to work on a single image without the need for temporal information. However, static approaches can also be applied to a video sequence where each frame is analyzed independently, and a final decision on the video can be made by taking the majority decision. Generally, the static approaches are known for their good performance, low computation, and low cost. Furthermore, they are faster in comparison with dynamic schemes. Available state-of-the-art static approaches can be further divided into three main groups depending on the nature of the algorithm, namely, (1) texture-based approaches, (2) frequency-based approaches, and (3) hybrid approaches.

Texture-based approaches are based on analyzing microtextural patterns in the face image sample. This kind of approach is very successful in detecting photo and display artifacts, because this method can efficiently discriminate between artifact characteristics such as the presence of pigments (due to printing defects), specular reflection, and shade (due to a display attack). The most famous and most widely used approach is based on Local Binary Patterns (LBPs) [Maatta et al. 2011]. The LBP method was first explored in Maatta et al. [2011] for the photo print attack and was then extended successfully to address the replay video attack [Chingovska et al. 2012] on face recognition systems. LBP captures the local primitives that are due to the presence of pigments (from printers) or the change in reflectance or specular reflection caused by the quality variation of the artifacts. Figure 12 shows the illustration of the $LBP^{u2}_{8,1}$ obtained for the bona fide presentation image (Figure 12(a)), laser print photo attack (Figure 12(b)), inkjet print photo attack (Figure 12(c)), and display attack using an iPad (see Figure 12(d)). As can be observed from Figure 12, LBP can indicate a qualitative difference in the texture patterns that exist between bona fide presentation images and artifact face images. The more prominent visual differences can be observed for laser print artifacts, as this presentation attack instrument shows print defects in terms of pigment that are well exploited by the LBP. Similar observations can also be witnessed with the display attack using an iPad tablet. Since the display (or electronic screen) attack includes the screen, this will emit unwanted frequencies and will also include reflections on the screen that in turn can be captured by the face sensor. The use of LBP can clearly bring out these qualitative differences by properly encoding the specular reflections and unwanted frequencies, as shown in Figure 12(d). In order to further understand the popularity of the LBP approach for the benefit of face presentation attack detection, we also consider the case of a 3D mask obtained from www.thatsmyface.com,3DMaskFAce. Since the material used in a 3D face mask exhibits different textural patterns as compared to real skin, the LBP features are quite successful in capturing these variations. This illustration can justify the popularity of the LBP for face PAD.

Figure 13 shows the qualitative results of the $LBP^{u2}_{8,2}$ obtained for both a bona fide presentation image and a 3D mask presentation image. It can be observed that the LBP can successfully capture the changes in real skin texture and 3D face mask artifact. Thus, the qualitative results of LBP for different types of face artifacts demonstrate its applicability.

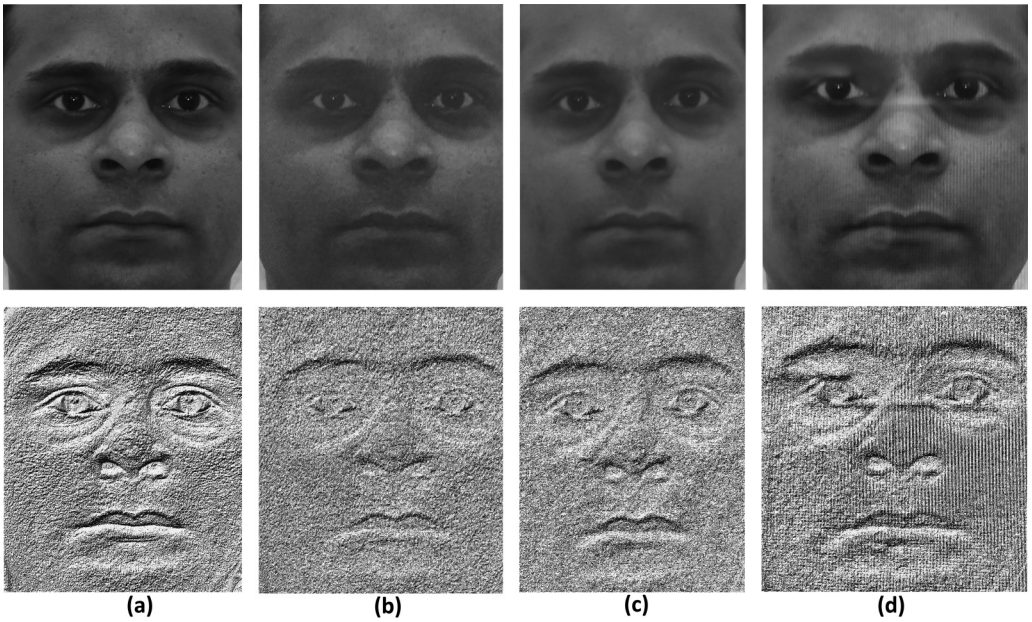

Fig. 12. Illustration of the effectiveness of LBP as a PAD: (a) bona fide image; (b) laser print artifact; (c) inkjet print artifact; and (d) display attack using iPad.

Fig. 13. Illustration of LBP on 3D mask attack: (a) face bona fide presentation and (b) 3D face mask presentation.

The first work on face PAD using LBP [Maatta et al. 2011] utilized three different LBP variants, namely, $LBP^{u2}_{8,1}$, $LBP^{u2}_{8,2}$, and $LBP^{u2}_{16,2}$, whose histograms are concatenated to form a single feature vector that in turn can be used to classify a presented face sample as an attack presentation or bona fide presentation. This approach has shown outstanding performance in detecting the photo print presentation attack on the face

Table IV. Brief Overview of Static-Texture-Based PAD Techniques

Reference	Techniques	Attacks	Database
Maatta et al. [2011]	LBP, LPQ, & Gabor	Photo attack	**Public**, 15 subjects
Chingovska et al. [2012]	LBP variants: LBP tLBP, dLBP, & mLBP	Replay video attack	**Public**, 50 subjects
Nesli and Marcel [2013]	LBP	3D mask video attack	**Public**, 17 subjects
Kose and Dugelay [2012]	LBPV	Photo	**Public**, 15 subjects
Kose and Dugelay [2012]	Component dependent descriptor	Photo & replay attack	**Public**, 15 subjects **Public**, 50 subjects
Raghavendra et al. [2015]	BSIF, CSLBP, & Contrast LBP (CLBP)	Photo	**Public**, 80 subjects
Raghavendra et al. [2015]	BSIF, CSLBP, & Contrast LBP (CLBP)	Display attack	**Public**, 80 subjects
Waris et al. [2013]	GLCM	Replay video	**Public**, 50 subjects
Yang et al. [2013]	Component dependent descriptor	Photo	**Public**, 50 subjects **Public**, 17 subjects
Raghavendra and Busch [2014c]	LBP & BSIF	Replay video & 3D face mask	**Public**, 50 subjects **Public**, 17 subjects
Waris et al. [2013]	Gabor & LBP LBP & GLCM Gabor & GLCM	Replay video	**Public**, 50 subjects
Raghavendra and Busch [2014c]	LBP & BSIF	Replay video & 3D face mask	**Public**, 50 subjects **Public**, 17 subjects

recognition system. This has motivated biometric researchers to further explore the effectiveness of the LBP feature extraction method on the replay attack. Extensive evaluation of LBP and its extended versions such as transitional LBP (tLBP) [Trefny and Matas 2010], direction-coded LBP (dLBP) [Trefny and Matas 2010], and modified LBP (mLBP) [Trefny and Matas 2010] for face PAD for the replay attack are presented in Chingovska et al. [2012]. Furthermore, the use of other LBP variants such as LBP variance (LBPV) [Zhenhua et al. 2010], Contrast LBP [Guo et al. 2010], and Center-Symmetric-LBP [Heikkilä et al. 2006] were also evaluated for both the photo and display screen attack in Raghavendra et al. [2015]. The effectiveness of the LBP and its variants was also further extended to detect 3D face mask presentation attacks [Nesli and Marcel 2013; Kose and Dugelay 2013a] on face recognition systems.

In addition to LBP and its variants, there are also various other texture-based methods for detecting 2D face penetration attacks. Table IV gives a brief overview of the most popular texture-based face PAD schemes. Even though it is very difficult to select one scheme over another, LBP and its variants can be found to be applicable. The use of micro-texture-based methods plays a substantial role in success, especially in detecting a print photo attack. However, combining one or more texture descriptors will further improve the reliability of face PAD approaches at the cost of computation.

The second type of static method includes techniques based on frequency analysis for the detection of face presentation attacks. The early work in this category was based on Fourier spectrum analysis [Li et al. 2004a] and was successfully used to detect the face photo attack. The same technique has been further extended to detect attacks using video replay by computing the Fourier spectra for head hair rather than a face

Table V. Brief Overview of Static Frequency-Based PAD Techniques

Reference	Techniques	Attacks	Database
Li et al. [2004a]	Fourier spectra & frequency dynamics descriptor (FDD),	Photo & video attack	Proprietary, 4 subjects
Weiwen [2014]	Fourier spectra	Video replay	Proprietary, 21 subjects
Peng and Chan [2014]	High-frequency descriptor	Photo print	Proprietary, 42 subjects
Teja [2011]	DCT energy	Photo print	Proprietary, 10 subjects
Zhang et al. [2012]	DoG	Photo print, wrap photo, & replay video	**Public**, 50 subjects

Table VI. Brief Overview of Static-Hybrid Schemes for Face PAD

Reference	Techniques	Attacks	Database
Galbally et al. [2014b]	Image quality	Photo print & video attack	**Public**, 50 subjects
Wen et al. [2015]	Image distortion analysis (IDA)	Print photo & replay video	**Public**, 110 subjects
Chingovska and Anjos [2015]	Client identity information	Print photo & replay video	**Public**, 50 subjects
Kim et al. [2015b]	Focus measure	Print photo	Proprietary, 24 subjects
Libin [2014]	Focus measure	Print photo	Proprietary, 42 subjects
Raghavendra and Busch [2014a]	2D Cepstrum & BSIF	3D mask	**Public**, 17 subjects
Määttä et al. [2012]	Texture & shape	Photo	**Public**, 17 subjects
Komulainen et al. [2013a]	Context	Photo & video	**Public**, 17 subjects
Gahyun et al. [2012]	LBP & 2DFFT	Photo	Proprietary, 25 subjects
Patel et al. [2015]	Moire pattern & shape deformation	Photo & video	**Public**, 1,000 subjects

[Weiwen 2014]. Furthermore, different techniques to quantify the frequency component are explored, including Discrete Cosine Transforms (DCTs) [Teja 2011], Difference of Gaussian (DoG) filters [Zhang et al. 2012], and high-frequency components [Peng and Chan 2014]. Table V gives a brief overview of the most popular frequency-based face PAD schemes. The third type of static approach includes hybrid schemes that combine more than one attribute [Galbally et al. 2014b; Wen et al. 2015], the use of client identity information [Chingovska and Anjos 2015], the characterization of the defocus property of the captured face image [Kim et al. 2015b; Libin 2014], one that combines time-frequency information with a texture descriptor [Raghavendra and Busch 2014a; Raghavendra et al. 2017], one that combines shape and texture [Määttä et al. 2012], or the use of context information [Komulainen et al. 2013a]. Table VI presents a brief overview of the static-hybrid schemes that are most widely used in face presentation attack detection. As can be seen from Tables IV, V, and VI, it is quite difficult to select the best among the available static techniques. However, based on the results achieved from the public databases, it is quite evident that texture-based methods have a greater impact on photo print detection and demonstrate outstanding performance, although in the case of video replay detection, the use of hybrid schemes appears to be an appealing choice.

Dynamic Approaches. The idea of a dynamic approach is to exploit the temporal information from the video replay presented to the face recognition sensor. Dynamic approaches tend to model this temporal information by exploiting the relative motion across the video frames. Hence, a dynamic approach will require more time as well as more computational effort when compared with a static approach. Existing

Table VII. Brief Overview of Dynamic Motion-Based PAD Techniques

Reference	Techniques	Attacks	Database
Wei et al. [2009]	Optical flow	Photo attack	Proprietary, 10 subjects
Bing-Zhong et al. [2010]	Optical flow	Photo attack	Proprietary, 4 subjects
De Marsico et al. [2012]	Head movement tracking	Photo attack	Proprietary, 20 subjects
Tao et al. [2013]	3D face structure by head movement	Photo attack	**Public**, 50 subjects
Anjos et al. [2014]	Optical flow correlation (OFC)	Photo attack	**Public**, 50 subjects
Younghwan et al. [2011]	Background motion index using GMM	Photo & display attack	Proprietary, 10 subjects
Junjie et al. [2012]	Motion estimation using GMM	Photo & display attack	**Public**, 10 subjects
Pinto et al. [2015]	Dynamic frequency as visual rhythms	Photo & display attack	**Public**, 50 subjects
Kollreider et al. [2009]	Optical flow lines	Photo & photo attack	Proprietary, 100 subjects

state-of-the-art dynamic approaches can be broadly be classified into three types: (1) motion based-approaches, (2) texture-based approaches, and (3) hybrid schemes.

The motion-based methods capture the subconscious motion exhibited by the muscles in the face due to the movement of the head. The captured motion is particularly due to the movements of the head [De Marsico et al. 2012; Anjos et al. 2014], mouth [Kollreider et al. 2007], or eyes [Gang et al. 2007].[3] The optical flow-based motion vectors for detecting subconscious head movements were introduced in Wei et al. [2009], and the optical flow-based motion extraction scheme was further explored by Bing-Zhong et al. [2010] to detect a photo attack that was presented with a great deal of artificial motion by swinging and bending, while bona fide presentations are normally recorded. The head movements were also explored for the detection of the photo-based presentation attack [De Marsico et al. 2012; Tao et al. 2013]. Context-based motion extraction to differentiate the face from the background is also explored in Anjos et al. [2014], Younghwan et al. [2011], and Junjie et al. [2012]. Furthermore, the use of dynamic frequency information as visual rhythms was introduced in Pinto et al. [2015]. Table VII presents a brief overview of the most relevant motion-based techniques used in face presentation attack detection.

The second type of motion-based scheme explores the dynamic texture change across the captured video. Early work in this direction is based on Local Binary Patterns from three orthogonal planes (LBP-TOP) [De Feitas Pereira et al. 2013] and has demonstrated a reasonable performance on the replay attack database [Chingovska et al. 2012].

The third approach explores both motion- and texture-based features to achieve highly accurate performance in identifying face presentation attacks. The use of multiple scenic cues was introduced in Junjie et al. [2012], exploring both motion- and texture-based features to identify a video replay attack on face recognition systems. Motion magnification using Eulerian video magnification (EVM) [Hao-Yu et al. 2012] along with various textural descriptors was introduced in Bharadwaj et al. [2013]. Table VIII presents existing hybrid schemes that have proven to be robust when compared to individual schemes. Table IX presents a summary of the advantages and limitations of software-based approaches.

[3]Since we have already discussed blink detection as a part of the hardware-based PAD scheme, the same techniques (for instance, motion computed using optical flow) can also be used provided this is performed subconsciously.

Table VIII. Brief Overview of Dynamic Hybrid-Based PAD Techniques

Reference	Techniques	Attacks	Database
Junjie et al. [2012]	Motion using GMM & Texture features	Replay video attack	**Public**, 50 Subjects
Bharadwaj et al. [2013]	EVM and HOOF	Replay video attack	**Public**, 50 Subjects
Komulainen et al. [2013b]	Motion & LBP	Replay video attack	**Public**, 50 Subjects

Table IX. Advantages and Limitations of Software-Based Approaches

Methods	**Advantages**	**Limitations**
Texture based	-Low computation cost -Effective on photo attack	-Lack of generalizability -Depends on image resolution
Frequency based	-Low computation cost -Less sensitive to face region -Effective to display attack	-Lack of generalizability -Device dependent
Hybrid based	-Generalizability (reasonably) -Effective to photo and display attack	-High computation cost
Motion based	-Provide the liveness measure -Effective on photo attack	-Lack of generalizability -High computation cost

Tables II through VIII provide a summary of the existing face presentation attack detection schemes. The idea of these tables is to present the existing approaches schematically in terms of the techniques and the corresponding database used. Since the performance evaluation of the state-of-the-art techniques described earlier is carried out using various error metrics and private databases, we have not reported the performance of each individual technique. However, we include the performance evaluation of the 14 different static software-based PAD algorithms in Section 8.

5. FACE ARTIFACT DATABASES

The availability of public databases plays an important role in developing new face PAD schemes and in reproducing the reported results. In this section, we provide details of all publicly available face PAD databases. There are eight large-scale face presentation attack databases, namely:

NUAA Impostor Database [Tan et al. 2010]

This is the first face presentation attack database that was made public. The whole database comprises 15 subjects whose bona fide face videos are recorded using a webcam. Each subject was recorded over three sessions, and each session contains 500 samples for each subject. The face artifact is generated by taking a high-quality face image for each subject using a DSLR camera, which is then printed on both photographic and 70g A4 paper using a color HP printer.

Yale-Recaptured Database [Peixoto et al. 2011]

This database is the result of recapturing the extended Yale Face Database B, which uses various illuminations. This database is more appropriate for evaluating the recapture detection algorithm, since the face artifacts are captured using two different high-resolution cameras by displaying the bona fide face samples using the LCD monitor. Since recapture uses illuminated faces, this database may not be suitable for a vulnerability analysis.

Print-Attack Database [Anjos and Marcel 2011]

This database is composed of 50 subjects whose bona fide face samples are captured using an Apple 13-inch MacBook laptop. The attack samples are generated by capturing the high-quality bona fide face image with both controlled and adverse conditions using a 12.1 megapixel Canon PowerShot SX150 IS camera. Then, these high-quality bona fide face images were printed on plain A4 paper using a Triumph-Adler DCC 2520 color laser printer and then presented to the camera with a hand-held and fixed setting. This is the first database of its kind that will allow one, on the one hand, to evaluate vulnerabilities, and on the other hand to develop new PAD schemes for more realistic conditions.

Replay Video Attack Database [Chingovska et al. 2012]

This database is an extension of the print-attack database [Anjos and Marcel 2011]; however, the attack samples are captured by replaying a video of a bona fide capture using an iPhone and iPad. This database provides a platform for developing face PAD algorithms targeted toward video replay attacks.

CASIA FAS Database [Zhang et al. 2012]

This database is similar to the replay video attack database [Chingovska et al. 2012] except that the attack samples are collected using three different resolutions (low, middle, and high resolution).

MSU-MFSD Database [Wen et al. 2015]

This database is similar to both the CASIA FAS database [Zhang et al. 2012] and the replay video attack database [Chingovska et al. 2012].

GUC Light Field Face Artifact Database (GUC-LiFFAD) [Raghavendra et al. 2015]

This database is collected using a Lytro light field camera and comprises 80 subjects. The attack samples are collected by capturing high-quality photos of bona fide presentations using a Canon EOS 550D DSLR camera with 18 megapixels, and these are further printed on both laser and inkjet printers to generate the face print artifacts. For the display attack, the high-resolution photos are presented to the light field camera. This database enables evaluation of depth information to design new face PAD schemes.

3D Mask Attack Database [Nesli and Marcel 2013]

This is the first publicly available 3D mask database. It comprises 17 subjects, whose 3D masks were provided by thatsmyface.com [Mask 2014]. Image capturing was carried out using a Kinect device to give both depth and color to the images.

MSU-MFD Database [Patel et al. 2015]

This is the extended version of the MSU-MFSD database [Wen et al. 2015], which is composed of 1,000 subjects with three different kinds of face artifacts: print photo, display photo, and video replay attack.

MS-Face Database [Chingovska et al. 2016]

This is the first publicly available multispectral face artifact database. The evaluation of the proposed method is carried out using a newly created multispectral spoof database [Chingovska et al. 2016]. The database consists of images captured from 21 unique subjects. The images are acquired using a new-generation CMOS sensor with high-resolution imaging [Chingovska et al. 2016]. The NIR images are obtained using

Table X. Brief Overview of Publicly Available Databases

Dataset	Sensor	Resolution	Attacks	Subjects
NUAA Impostor Database [Tan et al. 2010]	Webcam	640 × 480 pixels	Photo	15
Yale-Recaptured Database [Peixoto et al. 2011]	Kodak C813 8.2MP & Omnia i900, with 5MP	64 × 64 (after preprocess)	LCD screen	28
Print-Attack Database [Anjos and Marcel 2011]	Apple 13-inch MacBook	320 × 240	Photo video	50
Video Replay-Attack Database [Chingovska et al. 2012]	Apple 13-inch MacBook	320 × 240	Video replay using iPhone & iPad	50
CASIA FAS Database [Zhang et al. 2012]	Three different cameras	640 × 480 1280 × 720 1920 × 1050	Photo (wrap & cut) & video replay attack	50
MSU-MFSD Database [Wen et al. 2015]	MAC Book Air 13 inch & Google Nexus 5	640 × 480 & 720 × 480	Print photo & replay video attack	55[a]
GUC-LiFFAD Database [Raghavendra et al. 2015]	Light field camera	1080 × 1080	Photo (laser and inkjet) & display (iPad) attack	80
3D Face Mask Database [Nesli and Marcel 2013]	Kinect	640 × 480	3D mask video	17
MSU-MFD Database [Patel et al. 2015]	iPhone 6 & Google Nexus 5	5264 × 2448 & 720 × 480	Print photo, display photo, & replay video attack	1000
MS-Face Database [Chingovska et al. 2016]	Multispectral camera	1280 × 1024	Print photo	21
Oulu-NPU Database [Zinelabidine et al. 2017]	Six different smartphones	Six different resolutions	Print photo & replay video	55

[a]Only 35 subjects are available in the public version of this database.

NIR illumination with a bandpass filter centred at 800nm, to allow only the NIR component to pass. Furthermore, the authors carefully designed the database to capture the data under various imaging conditions [Chingovska et al. 2016]. In the bona fide dataset, each subject was captured in five different ways, in both the visible spectrum and the NIR spectrum independently. The artifact/spoof attack database was created by presenting three printed images of the best quality in the visible spectrum. In the case of the NIR attack database, images were printed in black and white with 600dpi and were presented back to the sensor. The images were then recaptured to create the artifact dataset under three conditions corresponding to a real-access data capture, which includes three different lighting conditions in an office environment: natural light, ambient light, and two spotlights.

Oulu-NPU Face Presentation Attack Database [Zinelabidine et al. 2017]

The Oulu-NPU face presentation attack database consists of 4,950 bona fide and artifact face videos corresponding to the 55 subjects. The bona fide samples were recorded using the front cameras of six mobile devices (Samsung Galaxy S6 edge, HTC Desire EYE, MEIZU X5, ASUS Zenfone Selfie, Sony XPERIA C5 Ultra Dual, and OPPO N3) in three sessions under different illumination conditions. The artifact species were collected using different types of PAIs, including two different kinds of printers and a display screen.

Table X provides an overview of the different face presentation attack databases that are available publicly. The reader can refer to the corresponding references to obtain the databases.

6. FACE PRESENTATION ATTACK DETECTION COMPETITIONS

In this section, we summarize the results of the face presentation attack detection competitions that were carried out during 2011 and 2013, respectively. These competitions provided a common platform in terms of datasets as well as evaluation protocols

Table XI. Brief Overview of Techniques Employed in the First Face PAD Competition

Team	Techniques Used	HTER (%)
AMILab	Texture, motion, & blink detection	0.63
CASIA	Texture, motion	0.00
IDIAP	Texture	0.00
SIANI	Motion	10.00
UNICAMP	Texture, motion, & blink detection	0.63
UOULU	Texture	0.00

Table XII. Brief Overview of the Techniques Employed in the Second Face PAD Competition

Team	Techniques Used	HTER (%)
CASIA	Texture & motion	0.00
IGD	Motion magnification	9.13
MaskDown	Texture & motion	2.50
LNMIT	Texture & motion	0.00
MUVIS	Texture	1.25
PRA Lab	Texture	1.25
ATVS	Image quality measures	12.00
UniCamp	2D Fourier spectrum & GLCM	15.62

and thus provide a trustworthy assessment of algorithms that were submitted to these competitions. The first face PAD competition was carried out during 2011 on the print attack database [Anjos and Marcel 2011] with six different competitors. Most of the algorithms are based on hybrid techniques, which include both textural features and motion. Table XI provides an overview of the techniques and the performance measures in terms of half total error rate (HTER%). Based on the performance achieved by different participants, the use of textural-based measures appears to be a valuable choice against a print photo attack.

The second face PAD competition was carried out during 2013, and eight different teams participated. This competition was carried out on the video replay database [Chingovska et al. 2012] and the performance measure was the HTER%. Table XII gives an overview of the techniques employed and the level of performance achieved. As can be noted from Table XII, the techniques employed by the participants are based on texture, frequency, image quality, motion, motion magnification techniques, and hybrid schemes that combine both textural and motion features. The best result is noted for the hybrid scheme, which combines both texture and motion features. All the results illustrated in Tables XI and XII are taken from Chakka et al. [2011] and Chingovska et al. [2013], and the reader can refer to these works for more information.

6.1. Discussion

The first face PAD competition was carried out on a database of 50 subjects, whose bona fide videos were captured using a QVGA sensor with a resolution of 320×240 pixels. The attack presentation videos were captured by presenting a photo of the subject printed using a color printer on A4 paper to the same sensor. The captured database had 200 bona fide videos and 200 artifact videos and was limited to an evaluation of the algorithms for the print photo video attack. This competition attracted six participants, of which five submitted an algorithm based on texture (and motion) analysis. Of the six algorithms provided, three demonstrated outstanding performance, with an error

rate of 0% (see Table XI). It is interesting to note that all three algorithms were based on texture analysis, primarily using LBP [Maatta et al. 2011]. It is also interesting to note that the degraded performance of the motion features resulted in an error of 10%. Thus, the primary outcome of this competition indicated the robustness of the texture-based approach using LBP in identifying a photo attack, as this can adequately capture the pigments (due to printing).

The second competition was carried out using the same database as for the first competition, but it was extended to include a new artifact corresponding to the video replay attack. In practice, the video replay attack is a very challenging method since it can overcome many liveness measures. Eight algorithms were submitted to this competition, which explored textural features, motion features, liveness measures, and hybrid approaches combining texture and motion. Of the eight algorithms submitted, two algorithms reported an outstanding performance with 0% error (see Table XII). Both of these highest-performing methods were based on a hybrid approach that combined the decisions from both texture- and motion-based methods. The texture-based approach was again based on the LBP [Maatta et al. 2011] (for both algorithms) and motion-based approaches including the Gaussian mixture model and optical flow, used independently in these two high-performing algorithms. The main outcome of this competition strongly indicates the generalizing capability of the hybrid approaches, although at a high computational cost.

7. PERFORMANCE EVALUATION METRICS

In this section, we present the PAD evaluation metrics proposed in ISO/IEC DIS 30107-3 [International Organization for Standardization 2016], which is based on the framework for PAD as defined in ISO/IEC 30107-1:2016 [ISO/IEC JTC1 SC37 Biometrics 2016]. ISO/IEC 30107-3 is currently available as a draft international standard (DIS). The metrics that are included in this paper are cited from the most recent version of ISO/IEC DIS 30107-3 (dated 10-13-2016). Since this draft standard is still under review, these metrics may be improved in the final versions. However, these PAD evaluation metrics are included to create awareness and to facilitate the transition to a uniform evaluation and reporting methodology for future work in this field, which will support the reproducibility of results. Governmental agencies involved in the standardization process intend to apply these metrics to operational systems, which indicates the relevance of adopting these early. Moreover, many academic papers have already adopted these metrics.

ISO/IEC DIS 30107-3 introduces three levels of PAD evaluation: (1) PAD subsystem evaluation: this level evaluates only a PAD system, which is either hardware or software based; (2) data capture subsystem evaluation: this will evaluate a data capture subsystem that may or may not include the PAD algorithms but is focused more on the biometric sensor itself; and (3) full-system evaluation: providing end-to-end system evaluation.

Metrics for PAD System Evaluation

The PAD subsystems are evaluated using two different metrics, namely [International Organization for Standardization 2016]: (1) attack presentation classification error rate (APCER), defined as the proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations at the PAD subsystem in a specific scenario, and (2) bona fide presentation classification error rate (BPCER), defined as the proportion of bona fide presentations incorrectly classified as presentation attacks at the PAD subsystem in a specific scenario.

The APCER for a given presentation attack instrument species (PAIS) shall be calculated as follows:

$$APCER_{PAIS} = 1 - \left(\frac{1}{N_{PAIS}}\right) \sum_{i=1}^{N_{PAIS}} (RES_i), \tag{1}$$

where N_{PAIS} is the number of attack presentations for the given presentation attack instrument PAI species [ISO/IEC JTC1 SC37 Biometrics 2016]. RES_i takes the value 1 if the ith presentation is classified as an attack presentation and a value of 0 if classified as a bona fide presentation.

The BPCER shall be calculated as follows:

$$BPCER = \frac{\sum_{i=1}^{N_{BF}} RES_i}{N_{BF}}, \tag{2}$$

where N_{BF} is the number of bona fide presentations. RES_i takes the value 1 if the ith presentation is classified as an attack presentation and value 0 if classified as a bona fide presentation.

Metrics for Data Capture Subsystem Evaluation

Data capture subsystem evaluations are based on biometric sensors that may or may not include a PAD subsystem. Hence, performance is measured based on whether the data capture subsystem successfully acquires a sample or not. Thus, the performance metrics for evaluating the data capture subsystem include:

—*Data capture attack presentation classification error rate (Data Capture-APCER)*: the proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations at the data capture subsystem in a specific scenario.
—*Data capture bona fide presentation classification error rate (Data Capture-BPCER)*: the proportion of bona fide presentations incorrectly classified as presentation attacks at the data capture subsystem in a specific scenario.

Metrics for Full-System Evaluation

Full-system evaluations include comparison subsystem results in addition to PAD subsystem and data capture subsystem results that can be interpreted in both verification and identification scenarios [International Organization for Standardization 2016]. These can be explained as follows:

—*Verification scenario:* The results are presented normally with FMR/FMNR with the bona fide samples. In the case of attack samples, the performance is measured using the*impostor attack presentation match rate (IAPMR)*, which is defined for a full-system evaluation of a verification system as the proportion of impostor attack presentations using the same PAI species in which the target reference is matched.
—*Identification scenario:* The results are presented normally with false-negative identification rate (FNIR)/false-positive identification rate (FPIR) with the bona fide samples [International Organization for Standardization 2006]. In the case of attack samples, the performance is measured using the*impostor attack presentation identification rate (IAPIR),* which in a full-system evaluation of an identification system is defined as the proportion of impostor attack presentations using the same PAI species in which the targeted reference identifier is among the identifiers returned or, depending on intended use case, at least one identifier is returned by the system.

8. PERFORMANCE EVALUATION

In this section, we present a common evaluation framework for evaluating widely used face PAD algorithms on the publicly available face-spoofing databases. The main challenge to be addressed before achieving a common evaluation framework is the selection of PAD algorithms from the pool of highly diverse algorithms available in the literature. For instance, it is challenging to reimplement hardware-based face PAD algorithms, since these are tailored to a specific type of hardware (e.g., the type of face capture camera). Hence, in this work, we limit the performance evaluation study to software-based face PAD techniques. In particular, we consider software-based static PAD algorithms that include both texture- and frequency-based PAD techniques. To this end, we examined 14 different state-of-the-art face PAD algorithms by considering their accuracy in detecting the 2D face presentation attacks, as reported in the literature. The 14 different state-of-the-art algorithms are (1) LBP-SVM [Chingovska et al. 2012]; (2) a combination of LBP8, 1-LBP8, 2-LBP16, and 1-SVM [Maatta et al. 2011]; (3) LBPV-SVM [Kose and Dugelay 2012]; (4) contrast LBP-SVM; (5) CSLBP-SVM; (6) mLBP-SVM; (7) IMQ-QDA [Galbally et al. 2014b]; (8) BSIF-SVM [Raghavendra and Busch 2014b]; (9) DoG-SVM [Zhang et al. 2012]; (10) 2DFFT-SVM [Li et al. 2004b]; (11) IDA-SVM [Wen et al. 2015]; (12) block LPQ-SVM [Benlamoudi et al. 2015]; (13) DCT Energy-SVM [Nesli and Marcel 2013]; and (14) GLCM-SVM [Li et al. 2013]. Considering the fact that each of these selected techniques was evaluated on a different database (including proprietary databases) and that the reported results are based on different metrics (HTER, equal error rate (EER), and true-positive rate (TPR)), we therefore evaluate in this section the performance of the 14 different methods using a single common protocol for evaluation and one database (which is public); we report the results in compliance with ISO/IEC metrics.

All of these state-of-the-art (SOTA) algorithms were reimplemented and evaluated following a common protocol on the CASIA face spoof database [Zhang et al. 2012]. We selected this database since it includes three different face artifacts (print, wrap, and display) collected using three different cameras, which results in three different imaging quality conditions: low quality, medium quality, and high quality. Furthermore, this database also has a performance evaluation protocol that divides the entire database into the two independent subsets of training and testing. For more information on this database, readers can refer to Zhang et al. [2012]. All the PAD techniques that are evaluated in this work are trained using the training partition, and performance is reported using the testing partition of the database. This database consists of video acquisitions. In order to effectively analyze the performance of the static PAD techniques, we decompose the videos into frames and evaluate the algorithms for each frame to measure the overall performance.

In this work, we follow the evaluation protocol of the CASIA database to report the performance of the face PAD algorithms. Since our interest is in measuring the performance of the PAD algorithms, we present the results following the ISO/IEC metrics (see Section 7) APCER and BPCER. Thus, lower values of both APCER and BPCER indicate better performance of the PAD algorithm. Table XIII shows the statistics of the images in the training and testing subsets of the CASIA face-spoofing database.

Table XIV indicates the quantitative results of the SOTA static PAD techniques on low-quality images from the CASIA face-spoofing database. These quality samples primarily represent the context of smartphone (front camera) and low-cost web cameras used in laptops and desktops for face-recognition-based access control. We present the results for three different kinds of face artifacts: print photo, wrap photo, and display screen (or electronic screen) attack. Based on the extensive experimental results, it can be noted that the PAD method based on LBP-SVM [Chingovska et al. 2012]

Table XIII. Statistics of CASIA Face-Spoofing Database

	Number of Images							
	Training				Testing			
Image Quality	Bona Fide	Print (S1)	Wrap (S2)	Display (S3)	Print (S1)	Wrap (S2)	Display (S3)	Print (S1)
Low	3,160	3,831	3,149	4,176	4,711	5,837	4,518	5,431
Medium	3,099	3,926	3,897	3,097	5,178	5,778	5,769	4,346
High	4,533	5,009	2,378	4,410	5,716	7,451	4,253	5,531

Table XIV. Performance of SOTA Static PAD Techniques on Low-Quality CASIA Face-Spoofing Database

	Print Photo		Wrap Photo		Display Screen	
Methods	APCER	BPCER	APCER	BPCER	APCER	BPCER
LBP-SVM [Chingovska et al. 2012]	**5.27**	**5.6**	**1. 21**	**4.41**	**0.71**	**4.28**
LBP8,1-LBP8,2-LBP16,1-SVM [Maatta et al. 2011]	9.64	13.18	15.8	21.14	2.26	11.28
LBPV-SVM [Kose and Dugelay 2012]	12.23	23.24	15.75	24.43	4.86	18.4
Contrast LBP-SVM [Guo et al. 2010]	9.98	18.63	22.06	19.86	3.01	13.2
CSLBP-SVM [Heikkilä et al. 2006]	9.78	34.62	15.42	23.17	10.47	28.14
mLBP-SVM [Chingovska et al. 2012]	19.29	18.21	22.24	25.04	2.35	14.49
IMQ-QDA [Galbally et al. 2014b]	22.12	17.38	21.72	20.42	12.42	5.72
BSIF-SVM [Raghavendra and Busch 2014b]	5.85	20.18	14.03	8.29	2.75	15.47
DoG-SVM [Zhang et al. 2012]	12.48	44.59	24.85	23.45	12.33	13.03
2DFFT-SVM [Li et al. 2004b]	11.56	85.99	13.28	53.15	7.14	63.74
IDA-SVM [Wen et al. 2015]	14.88	8.72	10.06	28.37	0.83	24.2
Block LPQ-SVM [Benlamoudi et al. 2015]	5.28	9.19	3.09	5.2	0.93	5.51
DCT Energy-SVM [Nesli and Marcel 2013]	15.28	83.1	11.42	55.25	2.3	81.82
GLCM-SVM [Li et al. 2013]	0	94.29	0	94.29	98.95	5.68

indicates the best performance for all three kinds of artifacts. In particular, this method demonstrates outstanding performance for both the wrap and display attacks.

Table XV indicates the performance of the SOTA PAD schemes on medium-quality images from the CASIA face-spoofing database. These medium-quality images represent images from a CCTV camera, the back camera of a midrange smartphone, or the front camera of a high-end smartphone. Here we also present the results for three different kinds of artifacts such as print, wrap photo, and display attack. Based on the obtained results, the BSIF-SVM [Raghavendra and Busch 2014b] demonstrates the best results for the detection of all three types of face artifacts available in the CASIA database.

Table XV. Performance of SOTA Static PAD Techniques on Medium-Quality CASIA Face-Spoofing Database

	Print Photo		Wrap Photo		Display Screen	
Methods	APCER	BPCER	APCER	BPCER	APCER	BPCER
LBP-SVM [Chingovska et al. 2012]	1.86	11.2	16.95	5.42	7.25	5.92
LBP8,1-LBP8,2-LBP16,1-SVM [Maatta et al. 2011]	7.42	8.07	11.85	5.77	8.55	14.85
LBPV-SVM [Kose and Dugelay 2012]	10.29	11.42	18.04	9.52	10.95	24.39
Contrast LBP-SVM [Guo et al. 2010]	8.53	10.13	12.32	7.22	8.74	14.17
CSLBP-SVM [Heikkilä et al. 2006]	4.63	38.27	10.08	21.88	8.39	23.44
mLBP-SVM [Chingovska et al. 2012]	13.27	9.73	9.11	7.26	9.8	12.36
IMQ-QDA [Galbally et al. 2014b]	17.47	11.23	17.86	21.22	9.72	14.52
BSIF-SVM [Raghavendra and Busch 2014b]	**5.2**	**6.12**	**6.08**	**5.63**	**4.57**	**6.33**
DoG-SVM [Zhang et al. 2012]	9.72	34.08	18.07	17.47	13.59	16.58
2DFFT-SVM [Li et al. 2004b]	9.44	95.92	27.09	70.58	2.18	96.36
IDA-SVM [Wen et al. 2015]	12.45	30.01	9.81	28.7	26.89	0.2
Block LPQ-SVM [Benlamoudi et al. 2015]	6.61	5.81	13.19	4.86	7.17	1.52
DCT Energy-SVM [Nesli and Marcel 2013]	9.15	96	36.93	52.81	3.91	68.25
GLCM-SVM [Li et al. 2013]	0	100	0	100	0	100

Table XVI indicates the performance of the SOTA face PAD scheme on high-quality face images from the CASIA face-spoofing database. The use of high-quality cameras typically represents the context of highly secured access control scenarios such as border controls. Here we also present the results from three different kinds of artifacts: print photo, wrap photo, and display attack. Based on the obtained results, it can be observed that no single algorithm can work equally well for all three different kinds of artifacts. It is seen that the block LPQ-SVM [Benlamoudi et al. 2015] approach demonstrates the best performance for the print photo and electronic display screen attacks, while IDA-SVM [Wen et al. 2015] shows the best results for the wrap photo attack.

Thus, based on the results obtained from this unified framework for evaluating 14 different static PAD algorithms, the main observations can be summarized as follows:

—No single PAD algorithm demonstrated the best outcome for all three face artifacts under three different imaging scenarios.
—The imaging quality, in terms of resolution, plays a vital role in deciding the performance of the face PAD method. Thus, the PAD algorithm giving the best results for low-quality images may not provide good results with high-quality images.
—The error rates of SOTA static PAD algorithms increase with the quality of the attack images.

Table XVI. Performance of SOTA Static PAD Techniques on High-Quality CASIA Face-Spoofing Database

Methods	Print Photo		Wrap Photo		Display Screen	
	APCER	BPCER	APCER	BPCER	APCER	BPCER
LBP-SVM [Chingovska et al. 2012]	12.25	17.54	21.04	1.88	9.27	1.36
LBP8,1-LBP8,2-LBP16,1-SVM [Maatta et al. 2011]	11.09	16.7	28.3	2.81	12.9	3.76
LBPV-SVM [Kose and Dugelay 2012]	23.6	41.35	17.47	39.43	12.69	13.43
Contrast LBP-SVM [Guo et al. 2010]	16.53	10.35	20.66	7.64	14.24	3.72
CSLBP-SVM [Heikkilä et al. 2006]	18.96	55.36	55.46	17.77	22.96	25.73
mLBP-SVM [Chingovska et al. 2012]	9.7	20.41	14.5	16.16	4.67	14.73
IMQ-QDA [Galbally et al. 2014b]	18.46	12.91	12.42	17.12	8.76	12.47
BSIF-SVM [Raghavendra and Busch 2014b]	12.88	49.44	55.42	7.01	22.31	15.2
DoG-SVM [Zhang et al. 2012]	26.22	48.33	56.03	6.56	48.43	16.39
2DFFT-SVM [Li et al. 2004b]	2.13	86.33	2.13	86.33	12.74	26.13
IDA-SVM [Wen et al. 2015]	1.22	29.02	**2.15**	**2.11**	13.95	20.44
Block LPQ-SVM [Benlamoudi et al. 2015]	**7.86**	**12.56**	20.85	1.92	**8.44**	**0.61**
DCT Energy-SVM [Nesli and Marcel 2013]	1.34	93.68	0.02	93.77	12.33	26.13
GLCM-SVM [Li et al. 2013]	0	96.92	0	96.92	0	96.92

—Of the three different kinds of face artifacts, the print photo attack is slightly more difficult to detect using static PAD algorithms in comparison with the wrap photo and photo display attacks.

8.1. Discussion

It would be interesting to discuss the performance of various PAD algorithms achieved under the common evaluation framework compared with those reported in the state of the art. Even though a strict comparison is not feasible, an approximate comparison would be valuable in order to gain a better overview of the static face PAD techniques. To this extent, the following are the main observations:

—The performance obtained using the common evaluation framework gives the best results for LBP-SVM [Chingovska et al. 2012] on the three different artifacts captured at low resolution. A similar observation can also be noted with the results published in the state-of-the-art articles on both public and private databases. Furthermore, the outstanding performance of the LBP-SVM [Chingovska et al. 2012] is also acknowledged in the first face presentation attack detection competition.
—With an increase in the quality of the captured image (which will also influence the quality of the artifact sample), the performance of the LBP-SVM [Chingovska et al. 2012] degrades. In the case of medium-quality image data, the BSIF-SVM

[Raghavendra and Busch 2014b] shows the best results, and the obtained results are in line with the reported results in Raghavendra and Busch [2014b]. For high-quality data, the techniques that explore color information using IDA-SVM [Wen et al. 2015] and the phase information using block LPQ-SVM [Benlamoudi et al. 2015] give the best results. Since the results presented for IDA-SVM [Wen et al. 2015] on the CASIA database are reported using completely different metrics and also do not compare the performance of IDA-SVM [Wen et al. 2015] with the block LPQ-SVM [Benlamoudi et al. 2015], this makes it difficult to compare the results reported in the state of the art.

—Another important observation concerns the frequency-based techniques based on 2DFFT-SVM [Li et al. 2004b], DCT Energy-SVM [Nesli and Marcel 2013], and GLCM-SVM [Li et al. 2013]. These techniques were reported to show a low error rate of 0% on the private databases in their corresponding papers. However, these techniques show the worst performance, with very high error rates in our evaluation.

—Another observation on the IMQ-QDA [Galbally et al. 2014b] that is reported as the generalizable techniques across different artifacts also indicates the degraded performance in our evaluation. The degraded performance of IMQ-QDA [Galbally et al. 2014b] is also acknowledged in the second face presentation attack competition.

9. IDENTICAL TWINS: A CASE STUDY FOR FACE PRESENTATION ATTACK

In this section, we present a preliminary study of identical twins in order to analyze the vulnerability of the commercial face recognition system. The face recognition of identical twins is well explored by the face recognition community [Phillips et al. 2011; Vipin et al. 2011]. The available results indicate that accurately distinguishing identical twins, especially in the less constrained scenario, is very challenging. Thus, identical twins can be considered as a special case of a human face presentation attack. The possible vulnerability is that one of the twins can attack the face recognition system to gain access and to impersonate the other twin. Furthermore, twins can easily overcome the liveness and/or presentation attack detection methods since their attack is based on a living human presentation attack instrument.

We collected a pair of face images of twins and evaluated these samples using the VeriLook face recognition available from NeuroTech. We collected the twin face samples in a studio setting to capture high-quality face samples. The images were captured in three different sessions over 2 days. Figure 14 shows examples from the twin pair used in this work.

Table XVII indicates the quantitative results obtained using the VeriLook face recognition system. Based on the obtained results, we can see that the magnitude of the impostor comparison scores between twin subjects is small, as opposed to the magnitude of the genuine comparison score achieved from the within-subjects comparison. Based on the results obtained using the VeriLook face recognition system, the use of twins did not demonstrate a significant impact, especially for the presentation attack. On the contrary, the literature indicates high rates of false matches. Thus, this problem is critically important and requires a more detailed study.

10. CHALLENGES AND OPEN ISSUES

The topic of face presentation attack detection has received intensive research effort in terms of studying the vulnerability of face recognition systems to various face artifacts and developing various PAD techniques to detect these artifacts. In spite of these efforts, there are still several challenges and open issues that need to be addressed. In the following, we present challenges and open issues in the field of face presentation attack detection.

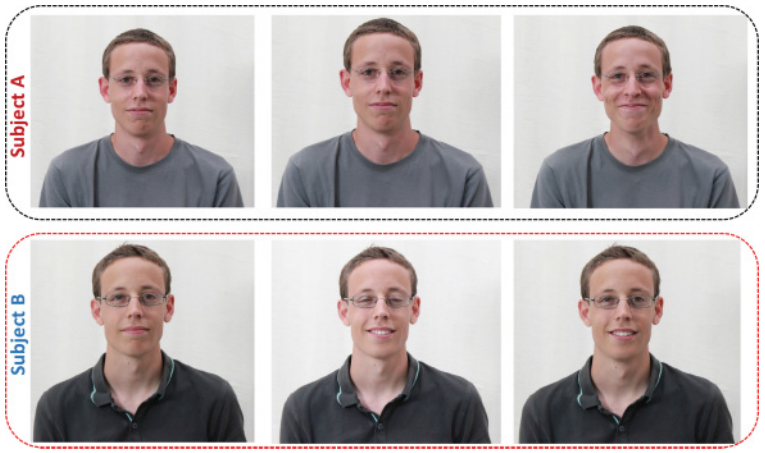

Fig. 14. Example of twin pair used in this analysis.

Table XVII. VeriLook Face Recognition Evaluation of Identical Twins

Reference	Probe	Comparison Score
Subject A Sample 1	Subject A - Sample 2	**431**
	Subject A - Sample 3	**732**
	Subject B - Sample 1	34
	Subject B - Sample 2	70
	Subject B - Sample 3	19
Subject B Sample 1	Subject B - Sample 2	**526**
	Subject B - Sample 3	**424**
	Subject A - Sample 1	34
	Subject A - Sample 2	26
	Subject A - Sample 3	27

Generalization for Various Artifacts

One very important issue that needs to be addressed is the generalization capacity of the existing face PAD techniques. Since the available PAD techniques are tailored to work with known attacks, it is not clear how they perform for unknown attacks. Moreover, the majority of the available face PAD schemes are learning based, with the intention of learning the decision policy for a subset of known attacks. This imposes a further challenge to improve the robustness of these learning techniques to unknown attacks or with unknown face artifacts. Even though recent work [Wen et al. 2015] has addressed this issue, the performance achieved by well-known face PAD techniques for unknown attacks is far from their application to real time. Another important aspect to be considered is the study of face PAD with respect to aging and ethnicity. With rapidly advancing technology, it is very easy to generate face artifacts with different ages and ethnicities. Figure 15 shows 3D mask images with varying ages and ethnicities that can be obtained from www.thatsmyface.com [Mask 2014]. Furthermore, a change in the environmental conditions and quality of the face artifacts will further challenge the existing PAD techniques in terms of robustness. As all possible types of attack or face artifact cannot be foreseen, one promising approach may be based on exploring the liveness features (e.g., estimating blood flow, exploring face veins, or using physiological signals).

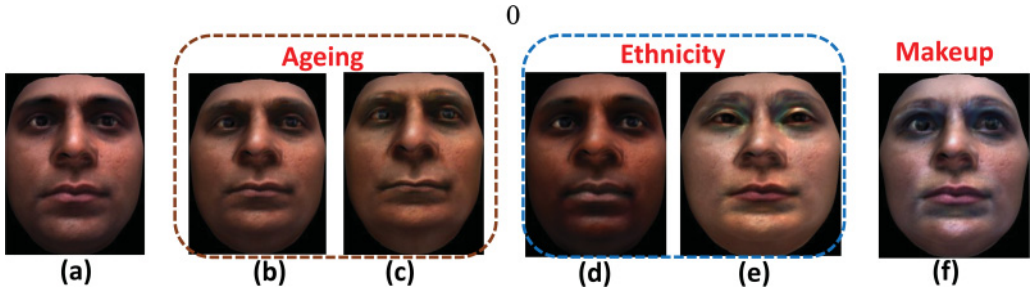

Fig. 15. Illustration of challenging face artifacts: (a) 3D face mask; (b) age variation of 10 years; (c) age variation of 40 years; (d) African ethnicity; (e) East Asian ethnicity; and (f) makeup.

Reporting the Performance

Despite the fact that face presentation attack detection has been investigated for more than a decade now, there is only a slow convergence toward harmonized testing and reporting. The most widely used metric is the HTER [Chingovska et al. 2014], which is the average of FRR (ratio of incorrectly rejected genuine score) and FAR (ratio of incorrectly accepted zero-effort impostor). However, FAR is also associated with SFAR (ratio of incorrectly accepted spoof attacks). Moreover, other work has measured the reliability of a PAD system by simply presenting the EER. The results published to date are therefore hard to compare. This illustrates the requirement for a common evaluation metric that is incorporated by both practitioners and researchers working on face PAD. The availability of an international standard using ISO/IEC was discussed in Section 7. This section provides valuable information about the standardized metrics that should be used when presenting the results of face PAD algorithms.

Interdependency Between PAD and Face Recognition System

There is a need to study the interdependency between PAD and face recognition (or baseline algorithm) units in the whole system. Most of the available PAD systems will work as a stand-alone unit that independently casts a decision about the presented face sample as a bona fide presentation or attack presentation. Since these PAD systems are also associated with errors, this may impact directly on the increased false non-match rate (FNMR) of the face recognition system. Thus, it is necessary to design an efficient fusion framework that can effectively combine the decision from the PAD unit with a face recognition unit. There has already been initial progress in this direction, performing this fusion by combining a comparison of the scores of the PAD system with a face recognition system in Chingovska et al. [2014]. However, a systematic study of the influence of different artifacts and its comparison scores on the face recognition unit needs to be addressed. Furthermore, there is also a need to adopt PAD systems to work in the context of the open identification (or watch-list) scenario.

Databases and Evaluation

Although there are several publicly available face PAD databases for the research community, these have many shortcomings, for example:

—Available databases are limited in terms of the number of subjects and types of attack. This will certainly limit the research community in reporting the performance of face PAD algorithms up to a level that is statistically significant. There is an attempt in this direction by Patel et al. [2015] to create a large face PAD database by collecting images from various web pages. Although this approach to setting up the database is very familiar, with face biometric research used to evaluate the performance of

face recognition algorithms, this approach may not be suitable for facial artifact generation. One possible reason for this is that images collected from web pages may be of varying quality or digitally altered, which may bias the experimental results of this database. This gives rise to a need for the creation of a large-scale database with a diverse selection of attacks and the exploration of different materials for generating face artifacts of sufficiently high quality to reflect their practical applications.

—Only a couple of publicly available databases have provided the evaluation protocol by partitioning the whole database into three disjoint sets for training, testing, and development. Apart from these few databases, other publicly available face PAD databases provide only two disjoint sets, for training and testing. This will introduce additional bias into the reported results for state-of-the-art PAD algorithms since the use of the training database for both tuning (parameters) and training simultaneously may result in the overfitting of the binary classifier used for PAD classification. Thus, these issues need to be considered when evaluating face PAD techniques.

Identical Twins

As discussed in Section 8, a detailed study of identical twins and their impact on the vulnerability of face recognition systems is urgently required. The performance of a systematic study analyzing the vulnerability of face recognition systems to identical twins on a large-scale database is needed.

User Convenience

The design of user-convenient (or user-friendly) PAD systems plays a crucial role in making them deployable in real-time applications. Thus, there is a need to design face PAD systems that allow minimum user intervention. This fact needs to be considered when designing a challenge-based response system.

11. CONCLUSION

The vulnerability of face recognition systems to low-cost artifacts such as photo print or video replay attacks indicates the resilience of face recognition systems to presentation attacks. To this end, a substantial number of face presentation attack detection algorithms are presented. In this article, we present a comprehensive review of publicly available databases and the relevant standards that define the performance metrics, and report the performance of face PAD algorithms. Finally, we also discuss the open issues and challenges that remain to be addressed. Even though there exist a large number of techniques to address various kinds of face artifacts, there is still a need to design a robust face PAD system that can be generalized to different face artifacts. Overall, this article can serve as a quick reference for face presentation attack detection techniques for both newcomers andexperts.

REFERENCES

A. Adler and S. A. C. Schuckers. 2015. Security and liveness, overview. *Encyclopedia of Biometrics* 1 (2015), 1335–1342.

A Ali, F. Deravi, and S. Hoque. 2013. Directional sensitivity of gaze-collinearity features in liveness detection. In *4th International Conference on Emerging Security Technologies (EST'13)*. 8–11.

A. Anjos, M. M. Chakka, and S. Marcel. 2014. Motion-based counter-measures to photo attacks in face recognition. *IET Biometrics* 3, 3 (Sept. 2014), 147–158.

A. Anjos and S. Marcel. 2011. Counter-measures to photo attacks in face recognition: A public database and a baseline. In *International Joint Conference on Biometrics (IJCB'11)*. 1–7.

A. Anjos, L. El Shafey, R. Wallace, M. Günther, C. McCool, and S. Marcel. 2012. Bob: A free signal processing and machine learning toolbox for researchers. In *20th ACM Conference on Multimedia Systems (ACMMM'12)*. ACM Press.

BEAT. 2010. Biometrics Evaluation and Testing (BEAT). Retrieved from https://www.beat-eu.org/.

S. Benlamoudi, A. Ouafi, A. Benlamoudi, T.-A. Abdelmalik, and A. Hadid. 2015. Face spoofing detection using multi-level local phase quantization (ML-LPQ). (2015).

S. Bharadwaj, T. Dhamecha, M. Vatsa, and R. Singh. 2013. Computationally efficient face spoofing detection with motion magnification. In *IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW'13)*. 105–110.

T. N. Bhaskar, F. T. Keat, R. Surendra, and Y. V. Venkatesh. 2003. Blink detection and eye tracking for eye localization. In *Conference on Convergent Technologies for the Asia-Pacific Region (TENCON'03)*, Vol. 2. 821–824.

J. Bing-Zhong, P. Chan, W. Ng, and D. Yeung. 2010. Anti-spoofing system for RFID access control combining with face recogntion. In *International Conference on Machine Learning and Cybernetics (ICMLC'10)*, Vol. 2. 698–703.

BVAEG. 2010. Biometric Vulnerability Assessment Expert Group (BVAEG). Retrieved from http://www.biometricsinstitute.org/pages/biometric-vulnerability-assessment-expert-group-bvaeg.html.

M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristori, F. Roli, J. Yan, D. Yi, Z. Lei, Z. Zhang, S. Z. Li, W. R. Schwartz, A. Rocha, H. Pedrini, J. Lorenzo-Navarro, M. Castrillón-Santana, J. Määttä, A. Hadid, and M. Pietikäinen. 2011. Competition on counter measures to 2-D facial spoofing attacks. In *2011 International Joint Conference on Biometrics (IJCB'11)*. IEEE, 1–6.

K. Chaudhury and A. Devarasetty. 2014. Liveness detection. US Patent 8,856,541. Retrieved from https://www.google.com/patents/US8856541.

I. Chingovska, A. Andr, and S. Marcel. 2012. On the effectiveness of local binary patterns in face anti-spoofing. In *Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG'12)*. 1–7.

I. Chingovska, J. Yang, Z. Lei, D. Yi, S. Z. Li, O. Kahm, C. Glaser, N. Damer, A. Kuijper, A. Nouak, J. Komulainen, T. Pereira, S. Gupta, S. Khandel Wa, S. Bansal, A. Rai, T. Krishna, D. Goyal, M. A. Waris, H. Zhang, I. Ahmad, S. Kiranyaz, M. Gabbouj, R. Tronci, M. Pili, N. Sirena, F. Roli, J. Galbally, J. Ficrrcz, A. Pinto, H. Pedrini, W. S. Schwartz, A. Rocha, A. Anjos, and S. Marcel. 2013. The 2nd competition on counter measures to 2D face spoofing attacks. In *2013 International Conference on Biometrics (ICB)*.

I. Chingovska, A. Andr, and S. Marcel. 2014. Biometrics evaluation under spoofing attacks. *IEEE Transactions on Information Forensics and Security (T-IFS)* 9, 12 (Dec. 2014), 2264–2276.

I. Chingovska and A. Anjos. 2015. On the use of client identity information for face anti-spoofing. *IEEE Transactions on Information Forensics and Security (TIFS)* 10, 99 (2015), 1–8.

I. Chingovska, N. Erdogmus, A. Anjos, and S. Marcel. 2016. Face recognition systems under spoofing attacks. In *Face Recognition Across the Imaging Spectrum*. Springer, 165–194.

B. M. Chrzan. 2014. Liveness detection for face recognition. *Master Thesis of Masaryk University.*

Cognitech. 2010. Cognitech: Face anti-spoofing discussion in find biometrics blog. Retrieved from http://findbiometrics.com/cognitecs-facevacs-entry-border-control-solution-ready-for-integration/.

Competition. 2013. The competition on counter measures to 2D facial spoofing attacks. Retrieved from https://www.tabularasa-euproject.org/evaluations/icb-2013-face-anti-spoofing.

Face COTS. 2015. Verilook COTS. Retrieved from http://www.neurotechnology.com/verilook.html.

C. Cunjian, D. Antitza, S. Thomas, and A. Ross. 2017. Spoofing faces using makeup: An investigative study. In *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA'17)*. IEEE, 1–8.

A. Dantcheva, C. Cunjian, and A. Ross. 2012. Can facial cosmetics affect the matching accuracy of face recognition systems? In *IEEE 5th International Conference on Biometrics: Theory, Applications and Systems (BTAS'12)*. 391–398.

T. De Feitas Pereira, A. Anjos, J. De Martino, and S. Marcel. 2013. LBPTOP based countermeasure against face spoofing attacks. In *Computer Vision (ACCV'12) Workshops*. Lecture Notes in Computer Science, Vol. 7728. Springer, Berlin, 121–132.

M. De Marsico, M. Nappi, D. Riccio, and J. Dugelay. 2012. Moving face spoofing detection via 3D projective invariants. In *5th IAPR International Conference on Biometrics (ICB'12)*. 73–78.

P. Dewan, D. M. Durham, L. Huang, K. S. Grewal, and X. Kang. 2013. Turing test based user authentication and user presence verification system, device, and method. WO Patent App. PCT/US2011/067,367. Retrieved from https://www.google.com/patents/WO2013100898A1?cl=en.

T. Dhamecha, R. Singh, M. Vatsa, and A. Kumar. 2014. Recognizing disguised faces: Human and machine evaluation. *PloS One* 9, 7 (2014), e99212.

N. M. Duc and B. Q. Minh. 2009. Your face is not your password. In *Black Hat Conference*, Vol. 1.

N. Erdogmus and S. Marcel. 2013. Spoofing attacks to 2D face recognition systems with 3D masks. In *International Conference of the Biometrics Special Interest Group*.

MORPHO Face. 2010a. Morpho face recognition. Retrieved from http://www.morpho.com/en/facial-recognition-0.

NEC Face. 2010b. Perturbation Space Method (PSM) for face spoof detection. Retrieved from http://www.nec.com/en/global/solutions/biometrics/technologies/face_recognition.html/.

Frontex. 2011. *BIOPASS II, Automated Biometric Crossing Systems: RAPID and SmartGate*. Vol. European Commission. Dictus Publishing.

Frontex. 2015. Best Practice Technical Guidelines for Automated Border Control (ABC) Systems. FRONTEX 2015.

K. Gahyun, E. Sungmin, S. Jae, K. Dong, P. Kang, and K. Jaihie. 2012. Face liveness detection based on texture and frequency analyses. In *5th IAPR International Conference on Biometrics (ICB'12)*. 67–72.

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

J. Galbally, S. Marcel, and J. Fierrez. 2014b. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. *IEEE Transactions on Image Processing* 23, 2 (Feb. 2014), 710–724.

P. Gang, S. Lin, W. Zhaohui, and L. Shihong. 2007. Eyeblink-based anti-spoofing in face recognition from a generic webcamera. In *IEEE 11th International Conference on Computer Vision, 2007 (ICCV'07)*. 1–8.

Z. Guo, D. Zhang, and D. Zhang. 2010. A completed modeling of local binary pattern operator for texture classification. *IEEE Transactions on Image Processing (TIP)* 19, 6 (June 2010), 1657–1663.

A. Hadid. 2014. Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions. In *IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW'14)*. IEEE, 113–118.

R. Hammoud. 2008. *Passive Eye Monitoring: Algorithms, Applications and Experiments*. Springer Science & Business Media.

W. Hao-Yu, R. Michael, S. Eugene, G. John, D. Frédo, and F. William. 2012. Eulerian video magnification for revealing subtle changes in the world. *ACM Transactions Graphics (Proceedings SIGGRAPH 2012)* 31, 4 (2012), 1–8.

M. Heikkilä, M. Pietikäinen, and C. Schmid. 2006. Description of interest regions with center-symmetric local binary patterns. In *Computer Vision, Graphics and Image Processing*. Vol. 4338. Springer, Berlin, 58–69.

Y. Hou, X. Hao, Y. Wang, and C. Guo. 2013. Multispectral face liveness detection method based on gradient features. *Optical Engineering* 52, 11 (2013), 113102–113102.

International Civil Aviation Organization NTWG. 2006. Machine Readable Travel Documents – Part 1 Volume 1 – Passports with Machine Readable Data Stored in Optical Character Recognition Format. http://www.icao.int/publications/pages/publication.aspx?docnum=9303.

International Organization for Standardization. 2006. *ISO/IEC 19795-1:2006. Information Technology - Biometric Performance Testing and Reporting – Part 1: Principles and Framework*. International Organization for Standardization.

International Organization for Standardization. 2016. *ISO/IEC DIS 30107-3:2017. Information Technology - Biometric Presentation Attack Detection - Part 3: Testing and Reporting*. International Organization for Standardization.

ISO/IEC JTC1 SC37 Biometrics. 2016. *ISO/IEC 30107-1:2016. Information Technology - Biometric Presentation Attack Detection - Part 1: Framework*. International Organization for Standardization.

E. John, S. Citard, and C. Busch. 2014. Detecting fingerprint alterations by orientation field and minutiae orientation analysis. In *International Workshop on Biometrics and Forensics (IWBF'14)*. 1–6.

S. U. Jung, Y. S. Chung, and K. Y. Moon. 2010. Method and apparatus for fake-face detection using range information. US Patent App. 12/509,825. Retrieved fromhttps://www.google.com/patents/US20100158319.

Y. Junjie, Z. Zhiwei, L. Zhen, Y. Dong, and S. Li. 2012. Face liveness detection by exploring multiple scenic clues. In *12th International Conference on Control Automation Robotics Vision (ICARCV'12)*.

KeyLemon. 2012. Keylemon face recognition tool. https://www.keylemon.com. Accessed 1-29-2014.

S. Kim, Y. Ban, and S. Lee. 2015a. Face liveness detection using a light field camera. *Sensors* 15, 1 (2015), 1537–1563.

S. Kim, Y. Ban, and S. Lee. 2015b. Face liveness detection using defocus. *Sensors* 15, 1 (2015), 1537–1563.

K. Kollreider, H. Fronthaler, and J. Bigun. 2008. Verifying liveness by multiple experts in face biometrics. In *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*. 1–6.

K. Kollreider, H. Fronthaler, and J. Bigun. 2009. Non-intrusive liveness detection by face images. *Image and Vision Computing* 27, 3 (2009), 233–244. Special Issue on Multimodal Biometrics Multimodal Biometrics Special Issue.

K. Kollreider, H. Fronthaler, M. Faraj, and J. Bigun. 2007. Real-time face detection and motion analysis with application in liveness assessment. *IEEE Transactions on Information Forensics and Security* 2, 3 (Sept. 2007), 548–558.

J. Komulainen, A. Hadid, and M. Pietikainen. 2013a. Context based face anti-spoofing. In *IEEE 6th International Conference on Biometrics: Theory, Applications and Systems (BTAS'13)*. 1–8.

J. Komulainen, A. Hadid, M. Pietikainen, A. Anjos, and S. Marcel. 2013b. Complementary countermeasures for detecting scenic face spoofing attacks. In *International Conference on Biometrics (ICB'13)*. 1–7.

N. Kose and J. Dugelay. 2012. Classification of captured and recaptured images to detect photograph spoofing. In *International Conference on Informatics, Electronics Vision (ICIEV'12)*. 1027–1032.

N. Kose and Jean Dugelay. 2013a. Countermeasure for the protection of face recognition systems against mask attacks. In *10th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG'13)*. 1–6.

N. Kose and J.-L. Dugelay. 2013b. On the vulnerability of face recognition systems to spoofing mask attacks. In *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'13)*. 2357–2361.

N. Kose and J.-L. Dugelay. 2013c. Reflectance analysis based countermeasure technique to detect face mask attacks. In *18th International Conference on Digital Signal Processing (DSP'13)*. 1–6.

A. Lagorio, M. Tistarelli, M. Cadoni, C. Fookes, and S. Sridharan. 2013. Liveness detection based on 3D face shape analysis. In *International Workshop on Biometrics and Forensics (IWBF'13)*. 1–4.

J. Li, Y. Wang, T. Tan, and A. Jain. 2013. Biometrics in ABC: Counter-spoofing research. In *FRONTEX 2nd Global Conference on Future Developments of Automated Border Control*. 296–303.

J. Li, Y. Wang, T. Tan, and A. K. Jain. 2004a. Live face detection based on the analysis of fourier spectra. *Proceedings of SPIE* 5404 (2004), 296–303.

J. Li, Y. Wang, T. Tan, and A. K. Jain. 2004b. Live face detection based on the analysis of fourier spectra. In *Defense and Security*. International Society for Optics and Photonics, 296–303.

Y. Libin. 2014. Face liveness detection by focusing on frontal faces and image backgrounds. In *International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR'14)*. 93–97.

R. Lindemann. 2014. System and method for eye tracking during authentication. US Patent App. 14/218,551. Retrieved from https://www.google.com/patents/US20140289834.

C. Liu. 2009. *Beyond Pixels: Exploring New Representations and Applications for Motion Analysis*. Ph.D. Dissertation. Citeseer.

J. Maatta, A. Hadid, and M. Pietikainen. 2011. Face spoofing detection from single images using micro-texture analysis. In *International Joint Conference on Biometrics (IJCB'11)*. 1–7.

J. Määttä, A. Hadid, and M. Pietikäinen. 2012. Face spoofing detection from single images using texture and local shape analysis. *IET Biometrics* 1, 1 (March 2012), 3–10.

Daily Mail. 2015. Real face spoofing case 1. Retrieved from http://www.dailymail.co.uk/news/article-1326885/Man-boards-plane-disguised-old-man-arrested-arrival-Canada.html.

S. Marcel, M. S. Nixon, and S. Z. Li. 2014. *Handbook of Biometric Anti-Spoofing*. Springer.

Biometric Market. 2015. Facial recognition market to reach 2.19bn dollars by 2019. *Biometric Technology Today* 2, 1 (2015), 2–3.

M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia. 2011. An evaluation of indirect attacks and countermeasures in fingerprint verification systems. *Pattern Recognition Letters* 32, 12 (2011), 1643–1651.

Face 3D Mask. 2014. 3D Face Mask. Retrieved from http://www.thatsmyface.com/.

MODI. 2015. MODI face recognition tool. Retrieved from http://www.modi-gmbh.de/en/product-detail/counterfeit-detection-2.

E. Nesli and S. Marcel. 2013. Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect. In *IEEE 6th International Conference on Biometrics: Theory, Applications and Systems (BTAS'13)*. 1–8.

Easy PASS. 2014. EasyPASS – Grenzkontrolle einfach und schnell. Retrieved from http://www.bundespolizei.de/DE/01Buergerservice/Automatisierte-Grenzkontrolle/EasyPass/_easyPass_anmod.html.

FAST PASS. 2012. FastPass- a harmonized, modular reference system for all European automated border crossing points. Retrieved from https://www.fastpass-project.eu.

K. Patel, H. Han, and A. K. Jain. 2015. *Secure Smartphone Unlock: Robust Face Spoof Detection on Mobile*. Technical Report MSU-CSE-15-15. Department of Computer Science, Michigan State University, East Lansing, MI.

B. Peixoto, C. Michelassi, and A. Rocha. 2011. Face liveness detection under bad illumination conditions. In *18th IEEE International Conference on Image Processing (ICIP'11)*. 3557–3560.

J. Peng and P. P. K. Chan. 2014. Face liveness detection for combating the spoofing attack in face recognition. In *International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR'14)*. 176–181.

J. Phillips, P. Flynn, K. Bowyer, R. Bruegge, P. Grother, G. Quinn, and M. Pruitt. 2011. Distinguishing identical twins by face recognition. In *IEEE International Conference on Automatic Face Gesture Recognition and Workshops*. 185–192.

A. Pinto, W. Schwartz, H. Pedrini, and A. Rocha. 2015. Using visual rhythms for detecting video-based facial spoof attacks. *IEEE Transactions on Information Forensics and Security* 10, 99 (2015), 1–9.

PRALAB. 2010. Open source software. Retrieved from https://pralab.diee.unica.it/en/FaceAntiSpoofingTool.

R. Raghavendra and C. Busch. 2014a. Novel presentation attack detection algorithm for face recognition system: Application to 3D face mask attack. In *IEEE International Conference on Image Processing (ICIP'14)*. 323–327.

R. Raghavendra and C. Busch. 2014b. Presentation attack detection algorithm for face and iris biometrics. In *22nd European Signal Processing Conference (EUSIPCO'14)*. 1387–1391.

R. Raghavendra and C. Busch. 2014c. Robust 2D/3D face mask presentation attack detection scheme by exploring multiple features and comparison score level fusion. In *17th International Conference on Information Fusion (FUSION'14)*. 1–7.

R. Raghavendra, R. Kiran, V. Sushma, C. Faouzi, and C. Busch. 2017. On the vulnerability of extended multispectral face recognition systems towards presentation attacks. In *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA'17)*. IEEE, 1–8.

R. Raghavendra, K. Raja, and C. Busch. 2015. Presentation attack detection for face recognition using light field camera. *IEEE Transactions on Image Processing* 24, 3 (2015), 1–16.

TABULA RASA. 2009. Trusted Biometrics Under Spoofing Attacks (TABULA RASA). Retrieved from https://www.tabularasa-euproject.org/.

R. K. Rowe. 2010. Comparative texture analysis of tissue for biometric spoof detection. US Patent 7,668,350. Retrieved from https://www.google.com/patents/US7668350.

D. Smith, A. Wiliem, and B. Lovell. 2015. Face recognition on consumer devices: Reflections on replay attacks. *IEEE Transactions on Information Forensics and Security* PP, 99 (2015), 1–9.

X. Tan, Y. Li, J. Liu, and L. Jiang. 2010. Face liveness detection from a single image with sparse low rank bilinear discriminative model. Lecture Notes in Computer Science, Vol. 6316. 504–517.

W. Tao, Y. Jianwei, L. Zhen, L. Shengcai, and S. Li. 2013. Face liveness detection using 3D structure recovered from a single camera. In *International Conference on Biometrics (ICB'13)*. 1–6.

M. H. Teja. 2011. Real-time live face detection using face template matching and DCT energy analysis. In *International Conference of Soft Computing and Pattern Recognition (SoCPaR'11)*. 342–346.

J. Trefny and J. Matas. 2010. Extended set of local binary patterns for rapid object detection. In *Computer Vision Winter Workshop*. 1–5.

M. S. Troy, R. C. Daley, and V. Yalla. 2014. System and method for structured light illumination with spoofing detection. US Patent App. 13/969,555. Retrieved from https://www.google.com/patents/US20140049373.

R. Unnikrishnan. 2014. Method and device for authentication of live human faces using infra red images. WO Patent App. PCT/US2013/058,677. Retrieved from https://www.google.com/patents/WO2014043003A1?cl=en.

V. Vipin, B. Kevin, F. Patrick, H. Di, C. Liming, H. Mark, O. Omar, S. Shishir, and K. Ioannis. 2011. Twins 3D face recognition challenge. In *International Joint Conference on Biometrics (IJCB'11)*. 1–7.

M.-A. Waris, H. Zhang, I. Ahmad, S. Kiranyaz, and M. Gabbouj. 2013. Analysis of textural features for face biometric anti-spoofing. In *2013 Proceedings of the 21st European Signal Processing Conference (EUSIPCO'13)*. 1–5.

B. Wei, H. Li, L. Nan, and J. Wei. 2009. A liveness detection method for face recognition based on optical flow field. In *International Conference on Image Analysis and Signal Processing*. 233–236.

L. Weiwen. 2014. Face liveness detection using analysis of Fourier spectra based on hair. In *International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR'14)*. 75–80.

D. Wen, H. Han, and A. Jain. 2015. Face spoof detection with image distortion analysis. *IEEE Transactions on Information Forensics and Security* 10, 99 (2015), 1–16.

M. Yamada and O. Yamaguchi. 2010. Image processing device, method and program. https://www.google.com/patents/WO2010137157A1?cl=en. WO Patent App. PCT/JP2009/059,805.

J. Yang, Z. Lei, S. Liao, and S. Z. Li. 2013. Face liveness detection with component dependent descriptor. In *International Conference on Biometrics (ICB'13)*. 1–6.

D. Yi, Z. Lei, Z. Zhang, and S. Z. Li. 2014. Face anti-spoofing: Multi-spectral approach. In *Handbook of Biometric Anti-Spoofing*, Sébastien Marcel, Mark S. Nixon, and Stan Z. Li (Eds.). Springer London, 83–102.

K. Younghwan, Y. Jang-Hee, and C. Kyoungho. 2011. A motion and similarity-based fake detection method for biometric face recognition systems. In *IEEE International Conference on Consumer Electronics (ICCE'11)*. 171–172.

Zhiwei Zhang, Junjie Yan, Sifei Liu, Zhen Lei, Dong Yi, and S.Z. Li. 2012. A face antispoofing database with diverse attacks. In *5th IAPR International Conference on Biometrics (ICB)*. 26–31.

Z. Zhang, D. Yi, Z. Lei, and S. Z. Li. 2011. Face liveness detection by learning multispectral reflectance distributions. In *IEEE International Conference on Automatic Face Gesture Recognition and Workshops (FG'11)*. 436–441.

G. Zhenhua, Z. Lei, and D. Zhang. 2010. Rotation invariant texture classification using LBP variance (LBPV) with global matching. *Pattern Recognition* 43, 3 (2010), 706–719.

B. Zinelabidine, K. Jukka, L. Li, X. Feng, and A. Hadid. 2017. OULU-NPU: A mobile face presentation attack database with real-world variations. In *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA'17)*. IEEE, 1–7.

Received April 2015; revised August 2016; accepted January 2017